
КРИСТОФЕР ХЭДНЕГИ
ИСКУССТВО ОБМАНА
СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В МОШЕННИЧЕСКИХ СХЕМАХ

КРИСТОФЕР ХЭДНЕГИ

ИСКУССТВО ОБМАНА

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В МОШЕННИЧЕСКИХ СХЕМАХ

альпина
ПАБЛИШЕР

Перевод с английского

Москва
2020

К русскому изданию

О чем эта книга, кратко можно сформулировать так: она об аналитической силе простых средств. Информация доступна, и с ее помощью можно сделать все что угодно. Доступность информации в сочетании с несложными манипулятивными приемами открывает любые двери.

В 1947 году, когда начиналась холодная война, основатель аналитической разведки Шерман Кент заявил, что в мирное время 80% данных для политических решений можно добыть в открытых источниках[1]. Уже выйдя на пенсию, бывший директор Разведуправления Министерства обороны США скорректировал эту оценку: 90% открытых источников и лишь 10% — агентурных операций[2]. Раньше пользовались газетами, журналами, ведомственными брошюрами, проспектами с выставок и телефонными справочниками. Сейчас все стало еще легче: к перечисленному добавились корпоративные сайты и социальные сети; смартфоны сопровождают фотографии геотегами, а для сбора данных о контактах любого человека достаточно просмотреть список его друзей.

Открытые источники дают огромную власть и одновременно делают вас крайне уязвимым. Информации из открытых источников достаточно, чтобы узнать об активном человеке почти все. Как? Однажды я потерял контакт с коллегой, с которым долго сотрудничал. Он удалил свою почту, профиль в Facebook и даже счет на PayPal. Но, когда потребовалось, я нашел его… по списку любимых книг. Можно сменить фамилию, переехать в другую страну и устроиться в международную организацию, но нельзя отказать себе в удовольствии отметиться под книгой, над которой работал. Сочетание русских и английских книг выдавало переводчика, а потом обнаружилось подтверждение — комментарий, в котором проскользнуло настоящее имя владельца аккаунта. Мы снова сотрудничаем, но мой коллега заволновался: только ли я смог проследить его связи со старой жизнью? Информация под руками, и все вполне законно — нужно лишь комбинировать данные.

В другом случае открытые данные пришлось сочетать с импровизацией. Моего приятеля, пожилого уже человека, обманули при покупке в интернете. Он перевел деньги по номеру телефона, после чего продавец попросту перестал отвечать на звонки. Мы перевели один рубль по тому же телефону, и через интерфейс онлайн-банка узнали его имя, отчество и первую букву фамилии. Затем я позвонил на тот же телефон через Skype:

— Иван Иванович, здравствуйте. Вас выбрали присяжным на процесс по делу о коррупции. Вы сможете явиться в Тверской городской суд послезавтра? Повестку мы пришлем.

— Но я живу в Туле.

— Вы ведь Иванов?

— Нет, я Петров.

— Простите, вечно у нас всё путают.

Мы нашли «Петрова» в соцсети, со всеми родственниками. Приятель по-стариковски обратился к его отцу. Тот оказался человеком понимающим, извинился, а через 15 минут извинялся сам незадачливый обманщик. Да,

мы имели дело с неопытным мелким мошенником, который не умел прятаться, но, во-первых, большинство из нас и не думает скрывать информацию о себе, а во-вторых, нельзя не пожалеть воришку — он показался мне таким беззащитным и в общем неплохим человеком.

Ну а вот дело посерьезнее. Работая с бухгалтерскими системами десять лет назад, мы не спрашивали пароли у владельцев рабочих мест: они были одинаковыми. Сегодня изощренные программы заставляют менять пароли и требуют фраз потруднее. Их трудно запомнить, но творческие бухгалтеры находят выход — они записывают пароли на обратной стороне клавиатуры. Злоумышленнику ничего не стоило проникнуть в нужный офис, устроившись на работу в клининговую компанию. Минимальная зарплата, текучка, уборщики меняются чуть ли не каждый день, да и кто замечает столь незначительного человека? А уж сфотографировать с экрана компьютера список крупных дебиторов — дело нескольких секунд. Простейшая разведка, дерзкая афера и банальная беспечность привели к невосполнимой потере рыночных позиций.

Читая «Искусство обмана», я переживал моральную коллизию. С одной стороны, автор учит использовать добро как слабость, тем самым обесценивая его. С другой — знание защищает. Описанные Кристофером Хэднеги методики сильны, но в то же время они и шаблонны. Как в фокусах иллюзиониста, их сила развеивается перед тем, кто знает секрет. Отрадно, что мошенники не умнее своих жертв, у них просто другие цели. Ввиду этого книга воспринимается совсем иначе. Она дает свободу совершать осознанные поступки, а не следовать манипуляциям, свободу ограничивать доступ к информации о себе, свободу частной жизни.

При редактирования перевода нам приходилось принимать решения о выборе слов для обозначения часто встречающихся терминов. В конечном счете он сводился к тому, предназначать ли книгу для узкого круга людей, тесно связанных с социальной инженерией, или делать ее понятной для всех. Мы выбрали второе. Надеемся на понимание читателей, для которых профессиональный жаргон стал родным — за «сбором данных из открытых источников» они узнают OSINT, за «легендой» — претекст и т.д.

Денис Букин,

психолог, психотерапевт,

автор книги «Развитие памяти по методикам спецслужб»

ОБ АВТОРЕ

Кристофер Хэднеги — генеральный директор компании Social-Engineer, LLC. Он ведущий разработчик и создатель первого систематизированного поискового интернет-ресурса, посвященного социальной инженерии, http://www.social-engineer.org. Хэднеги — основатель так называемой Деревни социальной инженерии (Social Engineering Village, или SEVillage) на конференциях DEF CON и DerbyCon[3] и разработчик популярной игры «Захват флага»[4], предназначенной для социальных инженеров (Social Engineering Capture The Flag — SECTF). Кристофер — востребованный во всем мире спикер и тренер: он выступал на таких мероприятиях, как RSA, Black Hat, DEF CON, и даже получал приглашение проводить консультации в Пентагоне. В Twitter он пишет под ником @humanhacker.

О техническом консультанте

Мишель Финчер — глава отдела информационной безопасности в химической компании. Уже больше 20 лет она занимается изучением человеческого поведения, а также является специалистом по информационной безопасности. Мишель специализируется на изучении психологических основ принятия решений, связанных с безопасностью, особенно в контексте социальной инженерии.

В роли тренера и спикера по различным техническим и поведенческим аспектам она выступала перед специалистами правоохранительных органов и разведки, а также в частном секторе, в том числе на таких мероприятиях, как Black Hat Briefings, RSA, SourceCon, SC Congress, Interop и Techno Security.

Мишель получила степень бакалавра в области проектирования с учетом человеческого фактора в Академии ВВС США, а также степень магистра в сфере консультирования в Обернском университете. Она является сертифицированным специалистом в сфере информационной безопасности (CISSP).

БЛАГОДАРНОСТИ

«Всего несколько лет назад мы с моим другом и учителем Мати Ахарони решили запустить сайт http://www.social-engineer.com» — такими словами начиналось первое издание книги «Искусство обмана: Социальная инженерия в мошеннических схемах». Сегодня, когда я перечитываю эти строки, мне кажется, что я сплю, вот-вот проснусь — и смутное воспоминание о том времени растворится. Я часто размышляю над тем, что случилось со мной за 12 лет, прошедших с выпуска того издания, и

особенно о событиях последних восьми лет, которые нашли отражение в этой книге.

За восемь лет мне довелось поработать с Полом Экманом, Робином Дрейке, Нилом Феллоном и прочими прекрасными людьми. Мне выпала честь брать интервью у Роберта Чалдини, Эми Кадди, Дова Бэрона, Эллен Лангер, Дэна Ариели и многих других выдающихся личностей. Мне посчастливилось выступать с Аполло Роббинсом и встретиться с Уиллом Смитом. Меня приглашали в Великобританию тренировать агентов MI5 и MI6. С точки зрения социальной инженерии я анализировал работу 35 генералов в Пентагоне, а также глав государств и других людей, обладающих властью.

Последние восемь лет были похожи на американские горки. Но, как говорится, один в поле не воин, так что этот опыт, удивительные знакомства и вся моя жизнь сложились именно так, а не иначе, благодаря людям, которые помогали мне. Моя жена Ариса — одна из самых терпеливых и прекрасных женщин, которых мне довелось встретить в жизни. И хотя ей чужд мир социальной инженерии, который стал для меня уже родным, она меня любит и всегда поддерживает. Благодаря Арисе моя жизнь полна смеха, приключений и счастливых воспоминаний.

Когда мой сын Колин был маленьким, он собирался стать врачом, потом писателем, а потом волонтером. Удивительно, он действительно попробовал себя в писательском деле и уходе за нуждающимися, а волонтерством занимается и сейчас. Его позитивный настрой и доброжелательность всегда были для меня примером.

Помню, как клялся: никогда близко не подпущу свою дочь Амайю к социальной инженерии: уж она-то будет жить в полной безопасности. Но Амайя ясно показала мне, что обеспечить ее безопасность я могу, только обучая своему делу и вовлекая в свою работу. Впрочем, она научила меня намного большему, чем я ее.

Хотя Пол Экман напрямую не участвовал в создании этой книги, его доброта, энтузиазм и щедрость меня очень вдохновили. Благодарю его за это.

Я также хочу поблагодарить всех людей, которые сопровождали меня на моем пути:

Пинг Лук — он всегда готов бескорыстно поддержать и помочь советом.

Дружба Дейва Кеннеди и его поддержка дали мне очень многое.

Хочу также поблагодарить членов фонда «Невинные жизни» (ILF) — они были неотъемлемой частью процесса.

Никогда бы не подумал, что мы с Нилом Фэллоном станем друзьями (ущипните меня). Но теперь он помогает мне, направляет и поддерживает меня. И главное — напоминает, что значит быть человеком.

ILF возник во многом благодаря поддержке и защите Тима Мэлони. Невозможно найти слова, чтобы выразить степень моей благодарности за его дружбу, веру и поддержку.

Энтузиазм Кейси Холл и ее стремление во что бы то ни стало найти решение, надо признать, очень заразительны.

Я благодарю Эй Джей Кук за помощь фонду и за то, как легко оказалось с ней работать. Ее преданность нашей общей цели спасения детей можно ставить в пример.

Профессиональная этика, доброта и способность сосредоточиться Аиши Тайлер делают ее примером для всех нас (даже ее имя кажется каким-то нереальным).

У меня в Social-Engineer, LLC, работает отличная команда. Колин, Майк, Кэт, Райан, Аманда, Каз, Джен и Карен — каждый из вас помог мне стать лучше и поддерживал меня. Спасибо!

Мне очень повезло с редактором этой книги, Шарлоттой. Иногда вообще казалось, что она может написать ее за меня — так легко Шарлотта понимала мои мысли и так умно помогала их выразить (вот уж работка, не позавидуешь!).

Читатели моих книг, ценители проекта Social-Engineer Podcast, посетители нашей Деревни SEVillage на конференциях и других мероприятиях, посвященных социальной инженерии! Благодаря вам моя планка поднялась очень высоко. Вы не боялись указывать мне на глупые ошибки и тем самым мотивировали меня постоянно развиваться. Благодарю!

ПРЕДИСЛОВИЕ

Когда в 1976 году мы со Стивом Джобсом основали Apple Computers, я и представить себе не мог, насколько это событие изменит мир. Тогда меня увлекла фантастическая идея: создать персональный компьютер, с которым мог бы самостоятельно работать отдельный пользователь. Прошло всего-то 40 с небольшим лет, а замысел уже давно воплотился в жизнь. По всему миру работают миллиарды ПК, смартфонов и других умных устройств, технологии проникли в самые разные аспекты нашей жизни. Теперь пришло время сделать шаг назад и подумать, как сохранить безопасность, не убивая при этом дух инноваций, продолжая развиваться и взаимодействовать с новыми поколениями.

Мне нравится работать с молодежью, вдохновлять ее на инновации и рост. Нравится смотреть, как загораются глаза молодых, когда у них появляются новые идеи и творческие решения по использованию технологий. Я просто обожаю следить за тем, как эти технологии улучшают нашу жизнь.

При этом я понимаю: для того чтобы будущее, которое мы строим, было безопасным, нужно потрудиться. В своей вступительной речи на конференции HOPE в 2004 году я говорил, что часто за компьютерными взломами стоит манипулирование: людей заставляют совершать весьма странные поступки. За годы работы в сфере безопасности мой друг Кевин Митник освоил искусство, которое принято называть социальной инженерией.

В книге Криса раскрыта суть социальной инженерии: это явление описано и разложено по полочкам в доступной форме. В новом издании также отражены принципы принятия решений и особенности манипулирования этим процессом.

Взломом компьютерных систем уже давно никого не удивишь, а манипуляции и вовсе существуют столько же, сколько и человечество. Эта книга научит вас обороняться от них, а также понимать и предотвращать связанные с социальной инженерией риски.

Стив Возняк

ВВЕДЕНИЕ

Я помню времена, когда в интернете по запросу «социальная инженерия» выпадали ссылки на видео о том, как получать бесплатно бургеры или заманить девушку на свидание. Сегодня же этот термин вошел в обиход и для краткости обозначается аббревиатурой СИ. Буквально на днях подруга нашей семьи (человек, бесконечно далекий от темы информационной безопасности) рассказывала о схеме мошенничества с использованием электронной почты. И резюмировала: «Согласитесь, отличный пример социальной инженерии!»

Я на секунду опешил. Но чему удивляться: восемь лет назад, когда я открыл компанию, сосредоточенную исключительно на социальной инженерии, это было в новинку, но сегодня СИ превратилась в полноценную отрасль.

Возможно, название этой книги могло сформировать у вас неправильное представление о моих намерениях: будто я собираюсь научить «плохих парней» воплощать в жизнь их дурные намерения. Но нет, это диаметрально противоположно истине.

Когда я взялся писать свою первую книгу, многие не одобряли эту затею: переживали, что я сослужу добрую службу недобрым людям. Но и тогда (как и сейчас) я понимал, что, прежде чем защищаться от социальной инженерии, надо разобраться во всех ее проявлениях. Ведь она как молоток, лопата, нож или пистолет. Каждый из этих предметов можно использовать для того, чтобы создавать, спасать, кормить, выживать. Но ими же можно калечить, убивать, разрушать. Чтобы понять, как использовать социальную инженерию в благих целях, нужно разобраться и с ее деструктивным применением. Это особенно актуально для тех, чья

задача — защищать. Чтобы уберечь себя и других от применения социальной инженерии во вред людям, нужно сначала заглянуть «на темную сторону».

Недавно я расспрашивал актрису Эй Джей Кук о ее работе в сериале «Мыслить как преступник». Она сказала, что в процессе подготовки к роли Джей-Джей не раз встречалась с реальными агентами ФБР, которые расследовали преступления серийных убийц. Так вот, моя книга написана по такому же принципу.

Читая ее, отбросьте предвзятость: я изложил все знания, опыт и практические наблюдения, которые собрал за последние десять лет работы в СИ. Конечно, здесь, как и в любой книге, могут обнаружиться ошибки. Возможно, какая-то информация вам не понравится или окажется не до конца понятной. Я всегда готов к дискуссии, только дайте знать! Найти меня можно на Twitter под ником @humanhacker. Или же пишите мне на электронные адреса, указанные на сайте http://www.social-engineer.org или http://www.social-engineer.com.

Когда я провожу пятидневный курс обучения СИ, то всегда прошу посетителей ни в коем случае не думать, будто я никогда не допускаю ошибок. Я только рад обсуждению, когда выясняется, что знания и соображения слушателей противоречат моим утверждениям, или если кому-то просто кажется, что я говорю не то. Я обожаю учиться, расширять и углублять понимание темы. Поэтому и вас прошу относиться к изложенной в книге информации критически.

Наконец, я хочу сказать вам спасибо. За то, что потратили свое бесценное время на прочтение этой книги. За то, что за последние годы вы помогли мне стать намного лучше. За обратную связь, идеи, критику и советы.

Надеюсь, книга вам понравится.

Кристофер Хэднеги

1 Заглянем в новый мир социальной инженерии

> Пожалуй, успех — это залог безопасности, а хороший вкус — залог успеха.
>
> Гордон Рамзи

Я отчетливо помню, как на экране моего компьютера появился первый абзац книги «Искусство обмана: Социальная инженерия в мошеннических схемах». Это было в далеком 2010 году. Так и хочется сказать, что в те древние времена рукописи набирались на печатной машинке, но так и быть, не стану драматизировать.

В те годы, введя в поисковую строку запрос «социальная инженерия», вы могли найти лишь пару страниц о самом известном специалисте в этой области, Кевине Митнике, да еще пару видео о том, как соблазнить

девушку или получить бесплатные бургеры в McDonald’s. Прошло восемь лет — и термин вовсю используется в повседневной жизни. В последние три-четыре года я неоднократно подмечал, как приемы из социальной инженерии используются в сфере безопасности, управления, образования, психологии, в военных организациях — словом, везде, где только можно представить.

Волей-неволей захочешь разобраться в причинах таких масштабных изменений. Один коллега сказал мне: «Так ты сам в этом виноват, Крис». Похоже, он говорил с укором, но я ощутил гордость. Впрочем, не один я несу ответственность за то, что сегодня повсеместно используется термин социальная инженерия. Полагаю, он вошел в обиход не только потому, что это самый простой способ атаки на системы безопасности различных компаний (как считалось семь лет назад), но и потому что сейчас атакующие получают самые большие прибыли. Себестоимость такой прибыльной атаки мала, риски — и того меньше. Окупаемость получается огромной. Моя команда собирает новости об атаках, проведенных с применением социальной инженерии, и связанную с ними статистику. И я с уверенностью могу сказать, что в 2017 году более 80% случаев взлома систем безопасности включали в себя тот или иной элемент СИ.

Согласно исследованию «Стоимости утечки данных», опубликованному IBM в 2017 году, из-за одной подобной утечки компании теряли порядка $3,62 млн. Понятно, почему мошенники с удовольствием используют СИ: ставки слишком высоки.

СОВЕТ ПРОФИ К 2017 году IBM выпускали такие исследования уже 12 лет подряд. Скачать последнее из них можно по ссылке https://www-03.ibm.com/security/data-breach/. Или же просто ввести в строку поисковика запрос: «IBM, стоимость утечки данных».

Помню первое интервью, которое я дал после публикации предыдущего издания этой книги в 2010 году. Меня спросили: «Не боитесь ли вы, что ваши советы возьмут на вооружение “плохие парни”?» Нет, не боюсь. Потому что отношусь к СИ как любому новому типу вооружения: все зависит от того, как его использовать.

В связи с этим мне вспоминается история, как в 1960-х Брюс Ли оказался в Америке. Тогда были сильны расовые предрассудки, а он взялся за дело, которым до него не занимался никто: обучал представителей всех рас, с любым цветом кожи, и национальностей древнему китайскому боевому искусству джиткундо. Он часто участвовал в турнирах со студентами своего университета. Те думали, что знают толк в драках, но Брюс, ко всеобщему удивлению, клал на обе лопатки одного соперника за другим. Многие из них потом стали его друзьями или учениками.

Для чего я привожу этот пример? Чтобы показать: людям пришлось адаптироваться к новому типу ведения борьбы, в противном случае они были обречены на поражение. Мог ли кто-то из учеников Брюса Ли

использовать полученные навыки, чтобы навредить другим людям? Конечно. Тем не менее Брюс передавал свои знания, потому что понимал: он должен учить людей защищаться.

Поэтому на вопрос, не боюсь ли я, что такая важная информация окажется на вооружении у «плохих парней», я отвечаю так же, как и восемь лет назад. Я не могу управлять тем, как читатели будут использовать полученные знания. Кто-то прочтет эту книгу и бросится применять описанные методы, чтобы красть деньги. А кто-то использует эти знания, чтобы защититься и для достижения благих целей. Ведь и «хороших парней» кто-то должен обучать. Одним словом, выбор за вами.

Чтобы противостоять противнику, владеющему новым стилем борьбы, недостаточно наловчиться принимать удары. Как и осваивая джиткундо, вам нужно будет разобраться в искусстве нападения и защиты, понимать, когда уместно одно, а когда — другое. Обучаясь социальной инженерии, придется научиться думать, как «плохие парни» (помня при этом, что вы к ним не относитесь). Раз уж я начал приводить аналогии, вот еще одна: нужно уметь использовать силу, но не переходить на темную сторону.

А сейчас вы, наверное, думаете: «Раз его мнение не изменилось, зачем он издает новую версию книги?». Сейчас расскажу.

Что изменилось?

Для социальных инженеров это фундаментальный вопрос. На первый взгляд кажется, что ничего особенно не меняется. Яркие примеры применения СИ можно найти даже в далеком прошлом. Например, самый древний из обнаруженных мной источников — это Библия, Книга Бытия (описанные в ней события происходили где-то в 1800 году до нашей эры). Иаков решил нечестным путем получить отцовское благословение, которое по праву первородства должно было достаться его старшему брату-близнецу Исаву. Иаков знал, что зрение их отца Исаака с годами ухудшилось и он больше полагался на другие органы чувств. Когда полуслепому Исааку нужно было понять, с кем из сыновей он общается, он полагался на обоняние, осязание и вкус. Иаков решил притвориться перед отцом Исавом. Он надел одежду старшего брата и приготовил еду так же, как тот. Но вот что самое интересное: Исав славился густым волосяным покровом, а Иаков был в этом смысле человеком вполне обычным. Поэтому он обмотал руки и шею шкурками молодых козлят. Это и решило дело: Исаак принял Иакова за Исава и отдал свое благословение младшему сыну вместо старшего. Так, согласно Книге Бытия, социальная инженерия помогла Исаву добиться желаемого.

В самых древних исторических документах мы видим, что люди постоянно хитрили, надували друг друга и жульничали — так что социальную инженерию никак нельзя назвать изобретением

современности. Но это не значит, что с течением времени она остается неизменной.

Взять хотя бы так называемый вишинг[5]. Помню, как я впервые использовал этот термин: на меня смотрели так, словно я заговорил на клингонском. Вот серьезно: как будто я сказал: «laH yIlo ’ ghogh HablI ’ HIv» (фанаты «Стартрека» оценят мои познания). Впрочем, в 2015 году слово «вишинг» благополучно пополнило Оксфордский словарь английского языка.

СОВЕТ ПРОФИ Хотя клингонский — выдуманный язык, существует вполне реальный институт (http://www.kli.org) для его изучения, а также для организации живого общения «носителей» этого языка. Можно найти и немало онлайн-переводчиков. Тем не менее о примерах использования социальной инженерии на клингонском я пока не слышал.

Итак, слово «вишинг» попало в словарь. Что такого? Дело в том, что это событие отражает силу влияния социальной инженерии на современный мир. Слово, которого раньше никто не знал, вошло в словарный запас большинства людей.

Но дело не только в словарном запасе. Сегодня существуют специальные сервисы, которые помогают злоумышленникам проворачивать свои махинации еще эффективнее. Например, работая с очередным клиентом, я наткнулся на сервис по проверке грамматических и других ошибок в фишинговых[6] e-mail: англоговорящие специалисты на службе у мошенников в режиме 24/7. Не будем также забывать, что в последние годы широкое распространение получила концепция использования сотрудниками собственных устройств на рабочем месте (BYOD), что большая часть мобильных гаджетов уже давно превратилась в мини-суперкомпьютеры, что современные люди зависимы от соцсетей… Все это создает плодороднейшую почву для проведения СИ-атак.

В общем, изменился мир, и я тоже. Первое издание книги «Социальная инженерия» я сопроводил подзаголовком «Искусство манипулирования людьми». На тот момент явление, которое я описывал в книге, действительно больше напоминало искусство — а оно, как известно, субъективно. Разные люди вкладывают в него разные смыслы, и чувства к нему можно питать тоже очень разные: от любви до ненависти, мотивированных чем угодно.

Второе издание книги называется «Искусство обмана: Социальная инженерия в мошеннических схемах». То, чем я занимался восемь лет назад, было для сферы обеспечения безопасности кардинально новым явлением. Я и сам учился ему в процессе работы. Но сейчас у меня гораздо больше опыта, и я могу с уверенностью сказать, что нахожусь в «состоянии познания».

Надеюсь, это мое состояние сделает книгу полезной вам, кем бы вы ни были: специалистом в области обеспечения безопасности, который

интересуется СИ, или энтузиастом, который не прочь расширить кругозор, а может — преподавателем, который хочет разобраться в теме и раскрыть ее своим ученикам. Не важно, кто вы, читатель. Но хочется верить, что научный подход к освещаемым вопросам позволит донести до вас информацию в полной мере и максимально эффективно.

Почему эту книгу стоит прочесть?

Мне кажется, первая глава этого издания должна быть написана по той же схеме, что и начало издания предыдущего. Поэтому хочу некоторое время уделить обсуждению того, почему я вообще считаю эту книгу достойной прочтения. Да, я понимаю, что до объективности мне в этом вопросе далеко, но все же позвольте высказаться.

Вы человек? Предположу: если вы сейчас читаете этот абзац, то вы либо продвинутая форма искусственного интеллекта, либо действительно человек. Осмелюсь даже заявить, что 99,9999999% читателей этой книги окажутся живыми людьми. Социальная инженерия изучает, как мы с вами устроены, чтобы найти уязвимые точки нашей системы принятия решений и эксплуатировать их.

Цель социального инженера — склонить вас к принятию необдуманных решений. Чем больше у вас будет возможностей обдумать происходящее, тем с большей вероятностью вы раскусите манипуляцию, а злоумышленникам этого, конечно, не надо. В седьмом и 70-м выпусках подкаста о социальной инженерии (The Social-Engineer Podcast, или «СИ-подкаст») мне выпала честь разговаривать с профессором психологии Гарвардского университета Эллен Лангер. Она рассказала мне о так называемых альфа- и бета-режимах работы мозга.

В альфа-режиме мозг генерирует волны с частотой колебания от 8 до 13 Гц (или циклов в секунду). Обычно для этого режима характерно состояние «грез наяву» или, как говорит профессор Лангер, «расслабленной концентрации».

ССЫЛКА НА СИ-ПОДКАСТ

Полные интервью Эллен Лангер можно послушать в нашем подкасте (на английском):

- В седьмом выпуске мы разговаривали с ней впервые — обсуждали ее исследования и книги: https://www.social-engineer.org/podcast/episode007-using-persuasion-on-the-mindless-masses/.
- 70-й выпуск мы записали пять лет спустя. Профессор Лангер вернулась в нашу студию, чтобы рассказать об изменениях за прошедшие годы: https://www.social-engineer.org/podcast/ep-070-thinking-with-out-a-box/.

Частота колебаний в бета-режиме варьируется от 14 до 100 Гц. В этом состоянии наш мозг находится в боевой готовности, максимально наблюдателен и полностью осознает происходящее вокруг нас.

Какой режим выгоднее для социального инженера? Конечно, альфа-режим: в нем человек меньше думает и не слишком внимателен. Причем используется этот режим не обязательно с целью навредить: например, существуют самые разные формы манипуляции и влияния, направленные на то, чтобы просто заставить вас действовать не раздумывая.

Например, вы наверняка хоть раз видели рекламу типа такой: на экране под очень грустную музыку появляется известная певица, затем нам показывают грязных, израненных, истощенных котят и щенков. Возникает ощущение, будто бедные зверюшки на волоске от смерти. Но тут вам снова показывают певицу, на этот раз в окружении здоровых животных, которых она с улыбкой гладит. Что все это значит? Всего за несколько долларов из вашего кошелька умирающие от голода котята и щенки превратятся в здоровых и счастливых. Кадр из такой рекламы вы найдете на илл. 1.1.

Можно ли утверждать, что создатели этой рекламы манипулируют вами ради наживы? Справедливости ради надо признать, что вряд ли удовлетворение собственных потребностей является единственной их целью. И все же они изучили и использовали методы воздействия на эмоции зрителя, чтобы тот с большей вероятностью пожертвовал деньги фонду или предпринял иное целевое действие. Такая манипуляция эмоциями, скорее всего, окажется успешнее, чем обращение к знаниям или логике. Чем сильнее эмоции, тем слабее становится наша способность рассуждать рационально. А уменьшение рациональности напрямую связано с ростом скорости принятия эмоциональных решений.

Изображение принадлежит Amazon Community Animal Rescue, http://www.flickr.com/photos/amazoncares/2345707195.

Илл. 1.1. Что вы чувствуете, глядя на это фото?

Так вот к чему я клоню. Если вы — человек, эта книга поможет вам разобраться, какие в принципе существуют типы СИ-атак. Вы узнаете, как «плохие парни» используют ваши человеческие качества против вас. Вы научитесь отражать их нападения, защищая в том числе своих близких.

И я предлагаю начать нашу большую и серьезную тему с обзора «Что же такое социальная инженерия?».

Социальная инженерия: обзор

Любое обсуждение социальной инженерии я обычно начинаю с определения, которое в почти неизменном виде использую последние 10 лет.

Но, прежде чем привести его здесь, я обязан сделать важное замечание: СИ — это сфера, где нет места политкорректности. Знаю, многие будут не в восторге, но это факт: социальные инженеры вовсю используют предрассудки, связанные с полом, расой, возрастом и социальным статусом людей, а также всевозможные комбинации этих предрассудков.

Например, представьте, что вам нужно проникнуть в здание, где расположилась компания клиента. Для этого понадобится убедительный предлог (или, как говорят в нашей сфере, легенда[7]): скажем, уборка помещений. В вашей команде собрались самые разные люди — кого из них лучше всего выбрать для исполнения роли уборщика?

- 40-летнего блондина;
- 43-летнюю азиатку;
- 27-летнюю латиноамериканку.

А если нужно подобрать человека для роли представителя компании, отвечающего за питание сотрудников?

- 40-летнего блондина;
- 43-летнюю азиатку;
- 27-летнюю латиноамериканку.

Конечно, если любой из перечисленных кандидатов является опытным социальным инженером, ему будет под силу любая роль. И все же чье появление вызовет у объекта воздействия меньше вопросов? Ведь никогда нельзя забывать: вопросы и размышления — главные враги социального инженера.

Так вот, помня об этом, давайте вернемся к определению СИ:

Социальная инженерия — это любые действия, подталкивающие другого человека сделать то, что может как пойти ему на пользу, так и навредить.

Почему я использую такое широкое, обобщающее определение? Потому что не считаю СИ явлением исключительно негативным.

Были времена, когда после заявления «Я — хакер» собеседники не разбегались от вас в ужасе, отключая на ходу все попадающиеся под руку электронные устройства. «Быть хакером» означало узнавать, как работает та или иная система. Ведь базовых знаний хакерам никогда не хватало, эти люди всегда копали глубоко, добираясь до сути. И, когда им открывалась вся картина, они видели способ обойти, улучшить или изменить исходную цель этой системы.

Работая над первой своей книгой, я стремился дать СИ такое определение, которое бы показало: этим делом далеко не всегда занимаются мошенники, воры и прочие преступники. Механизмы, которые используют злоумышленники, могут послужить и достижению благих целей. Это я и хочу донести до читателей.

Я часто привожу такой пример. Если бы вы подошли ко мне и сказали: «О, привет, Крис! Знаешь, я хочу поиграть с тобой в чаепитие для принцесс. Так что садись-ка на этот стульчик, надень розовый шарф, и, пока я буду красить тебе ногти, поговорим про героинь диснеевских мультиков», я бы над вами посмеялся, втихаря высматривая пути к

отступлению. Тем не менее в редких случаях я принимаю подобные предложения.

В каких? Например, не так давно именно это со мной проделывала моя дочка. И, прежде чем вы начнете возмущаться некорректности такого сопоставления (ведь я своего ребенка люблю, чего не сделаешь ради этого!), подумайте вот о чем. Да, я согласился играть в принцесс в первую очередь из-за любви к дочери, но ведь в процессе задействованы и другие психологические принципы. Чтобы сказать «да», мне за наносекунду нужно было обойти обычный процесс принятия решений, который в 99% случаев заставил бы меня отказаться от подобного предложения.

БЕСПОЛЕЗНЫЙ ФАКТ

Учитывая, что наносекунда — это одна миллиардная доля секунды, а среднестатистический человек говорит со скоростью порядка 145 слов в минуту, я физически не смог бы сказать «нет» за наносекунду. С другой стороны, скорость света составляет 299 792 км/с, а значит, за наносекунду свет преодолевает порядка 30 см.

После того как вы разберетесь в механизмах, задействованных в процессе принятия решений, вы начнете понимать, как злоумышленники используют эмоциональные триггеры и психологические принципы, на практике воплощая искусство и науку социальной инженерии. И все это — чтобы вы «предприняли действие, которое может вам навредить».

В 44-м эпизоде СИ-подкаста участвовал доктор наук, профессор Пол Зак, автор книги «Молекула морали» (The Moral Molecule; Dutton, 2012). В своей книге и в нашем подкасте он рассказывал об исследованиях процесса доверия и о роли в нем гормона под названием окситоцин. Доктор Зак озвучил очень важное для нас наблюдение: оказывается, когда мы чувствуем, что кто-то нам доверяет, в кровь выделяется окситоцин. Пожалуйста, отнеситесь к этой информации предельно серьезно. Ваш мозг выделяет окситоцин не только когда вы доверяете кому-то, но и когда вам кажется, что кто-то доверяет вам. Согласно исследованиям Пола Зака, этот феномен наблюдается не только при личном, но и во время телефонного или письменного общения, иными словами, даже когда вы не видите человека, который вам якобы доверяет.

ССЫЛКА НА СИ-ПОДКАСТ

В 44-м выпуске можно послушать увлекательнейшую беседу с Полом Заком о деле его жизни: http://www.social-engineer.org/podcast/ep-044-do-you-trust-me/.

Наш мозг производит и еще одно важное вещество — дофамин. Этот нейромедиатор выделяется в моменты удовольствия, счастья и получения положительной стимуляции. Смешайте окситоцин с

дофамином, и вы получите идеальный для социального инженера коктейль, который распахнет перед вами любые двери.

Дофамин и окситоцин обычно выделяются в мозге в процессе близкого общения, но это не обязательное условие. Цель социального инженера — создание располагающей к такому взаимодействию обстановки.

Я уверен, что мы, сами того не зная, применяем эти принципы ежедневно по многу раз: с супругами, начальниками, коллегами, священниками, терапевтами, обслуживающим персоналом — короче говоря, со всеми. А значит, понимание СИ и того, как выстраиваются процессы общения с другими людьми, важны для каждого из нас.

В мире, где в результате развития технологий мы научились общаться с помощью смайликов и сообщений, состоящих из менее чем 280 символов, нарабатывать навыки общения становится все сложнее. И уж совсем сложно выявлять ситуации, в которых эти навыки используются против нас. К тому же благодаря социальным сетям изменилось наше общество: стало нормальным и даже поощряемым рассказывать о себе абсолютно все всем подряд.

Итак, когда я говорю об использовании социальной инженерии в мошеннических целях, я обычно подразумеваю следующие направления деятельности:

СМС-мошенничество (SMiSHing), или фишинг с использованием текстовых сообщений. Когда в 2016 году атаке подверглась банковская компания Wells Fargo, я получил СМС-сообщение, скриншот которого изображен на илл. 1.2.

Перевод: **(wells_fargo)** *Важная информация от системы безопасности! Зарегистрируйтесь и прочтите => http://vigourinfo.com/secure.well5farg0card.html.*

Илл. 1.2. На эту удочку попались многие

Самое смешное, что я даже не пользовался услугами Wells Fargo и тем не менее якобы попал в список этой рассылки (и нет, названия своего банка я вам ни за что не выдам, даже не спрашивайте).

Всего один клик — и мошенники получали возможность собрать ваши идентификационные данные и/или загрузить на ваше мобильное устройство вирус.

Вишинг, или голосовой фишинг, о котором мы уже говорили выше. С 2016 года этот тип мошенничества стали применять намного чаще. Это простой, дешевый и очень выгодный для мошенников прием. Злоумышленников, использующих поддельные номера из других стран, практически невозможно найти и привлечь к ответственности.

Фишинг — самая обсуждаемая тема из мира социальной инженерии. Мы подробно писали о ней с техническим консультантом этой книги, Мишель Финчер, в другой нашей совместной работе — книге под названием «Темные воды фишинга: Нападение и защита» (Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails; Wiley, 2016). (Ладно, признаю, я только что беззастенчиво прорекламировал другую свою книгу.) С помощью фишинга закрывали целые заводы, взламывали системы числового программного управления (ЧПУ), обманывали системы безопасности Белого дома и десятков крупнейших корпораций, крали миллионы долларов. На данный момент фишинг считается самым опасным из четырех форм СИ.

Имперсонация[8], или подражание. Метод можно отнести к числу самых эффективных. А в конец этого списка он попал лишь потому, что отличается от остальных. Однако не стоит наивно полагать, будто вы не столкнетесь с ним в жизни. За последний год мы собрали сотни историй о том, как злоумышленники изображали полицейских, агентов федеральных служб или сотрудников еще каких-то ведомств, чтобы совершать поистине ужасные преступления. Например, в апреле 2017 года один из них попался на том, что выдавал себя за полицейского: сначала находил покупателей детского порно, а потом шантажировал их, пользуясь «служебным положением».

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

На момент публикации книги подробности этой отвратительной истории можно найти здесь (на английском): http://www.sun-sentinel.com/local/broward/pembroke-pines/fl-sb-pines-man-child-porn20170418-story.html.

Любой громкий случай СИ-атаки, который попадает в новости, можно отнести к одной из этих четырех категорий. В последнее время злоумышленники все чаще комбинируют эти методы для достижения максимальной эффективности.

Анализируя случаи подобных атак, я ищу в них общие схемы — не только для того, чтобы понять, какие инструменты и процессы задействовал преступник. Я стараюсь разобраться, как объяснить механизмы реализации атаки специалистам по безопасности, чтобы эту информацию можно было в дальнейшем использовать для саморазвития и защиты. Процесс анализа я выстраиваю по так называемой пирамиде СИ.

СИ-пирамида

Давайте я сразу объясню суть схемы, а уже потом расскажу, почему выделяю именно эти элементы и что означает каждый из них. Сама пирамида изображена на илл. 1.3.

Как видите, у нее есть нескольких ступеней и составлена она с точки зрения специалиста по безопасности, а не преступника.

Ниже я поясню общее значение каждой ступени пирамиды, а в дальнейшем, по ходу книги, мы будем разбирать их подробнее.

Илл. 1.3. Пирамида СИ

Сбор данных из открытых источников

Сбор данных из открытых источников[9] — фундамент деятельности социального инженера. На этот этап стоит закладывать больше всего времени при планировании атаки, поэтому он занимает первую и самую значимую ступень пирамиды. Однако одной из важных составляющих этого этапа редко достается должное внимание. Речь идет о подготовке документации: как следует записывать, хранить и каталогизировать собранную информацию? Подробнее мы обсудим этот вопрос в следующей главе.

Разработка легенды

Основываясь на данных, собранных из открытых источников, логично предпринять следующий шаг: начать разработку повода для атаки. Эта часть работы социального инженера должна основываться на собранной ранее информации. На этом этапе подготовки становится понятно, какие изменения и дополнения необходимо внести в исходный план атаки, а также какими дополнительными инструментами и реквизитом придется обзавестись.

План атаки

Проработкой легенды подготовка, конечно же, не ограничивается. Следующая стадия — планирование по модели трех «К»:

- Каков ваш план? Какова ваша цель? Какова цель клиента? Определившись с целями, вы легко ответите на следующие вопросы;
- когда лучше провести атаку;
- кто должен быть рядом на случай, если потребуется помощь?

Проведение атаки

Вот где начинается настоящее веселье. Завершив все этапы подготовки, вы сможете ринуться в бой. Вам нужно быть готовыми ко всему, но при этом не надо ограничивать свои действия слишком подробным сценарием. Я всегда рекомендую составлять план, потому что обычно это помогает сэкономить кучу времени и сил. Однако в плане не стоит описывать каждое движение — это только помешает вам, если случится какая-то неожиданность. Когда ваш мозг поймет, что сценарий вам больше не помощник, вы начнете запинаться и нервничать. Вы покажете свой страх, а это может помешать вам достигнуть цели операции. Поэтому я предлагаю писать не подробный сценарий действий, а скорее план, которому можно будет следовать, сохраняя творческую свободу.

Отчет

Погодите, не пролистывайте этот раздел! Прочитайте внимательно, о чем идет речь. Знаю, писать отчеты никто не любит. Но подумайте вот о чем: ваш клиент отстегнул вам кругленькую сумму за оказание неких услуг, с которыми вы, скорее всего, справились на ура. Но клиент платил вам не потому, что хотел казаться крутым. Он платил, чтобы вы разобрались, что надо делать с выявленной проблемой. Именно поэтому написание отчетов я поместил на вершину пирамиды — по сути, это кульминация, ради которой и нужны все предыдущие этапы.

Если последовательно выполнить каждый из описанных шагов, вас ждет успех не только как социального инженера, но и как специалиста по системам безопасности, который взял на себя обязательства перед клиентом. Потому что злоумышленники со всего света, занимающиеся социальной инженерией, готовят атаки по этой самой схеме. Только вот отчетов не составляют, конечно же.

В 2015 году на портале Dark Reading был опубликован материал об атаке, подготовленной по такой же пирамиде. (Прочитать этот текст на английском языке под названием «Соискатели атакуют: рассылка зараженных резюме» можно по

адресу: https://www.darkreading.com/vulnerabilities---threats/careerbuilderattack-sends-malware-rigged-resumes-to-businesses/d/d-id/1320236.)

1. Сначала, на стадии сбора данных из открытых источников, атакующие изучили возможные направления воздействия на объекты. Оказалось, что для этого был использован популярный сайт под названием Career Builder.
2. По завершении фазы сбора открытых данных злоумышленники перешли к разработке легенды. В результате появился образ претендента на вакансию, якобы готового устроиться на любую позицию в компании-объекте. Когда этот этап был пройден, стало понятно, какие инструменты потребуются в ходе атаки: зараженные файлы и правдоподобные резюме.
3. Злоумышленники начали планировать атаку, последовательно отвечая на каждый из приведенных выше «К»-вопросов.
4. В процессе атаки резюме были отправлены не объектам воздействия напрямую, а загружены на сайт Career Builder. Компании, которые публиковали там объявления о вакансиях, получали на электронную почту оповещения о появлении новых кандидатов. А к этим оповещениям прикладывались зараженные резюме.
5. Никаких отчетов атакующие не составляли, однако, благодаря деятельности специалистов компании Proofpoint, мы можем составить подробное представление об этапах их работы.

Успех этой атаки был связан в первую очередь с тем, что зараженный e-mail приходил жертвам с проверенного ресурса (Career Builder), так что люди открывали приложенные файлы без малейшего страха. А злоумышленники добивались именно этого: чтобы объект влияния совершил действие, противоречащее его интересам, не думая при этом о потенциальной опасности.

Что вы найдете в этой книге?

Составляя план этой книги, я старался сохранить структуру первого издания «Социальной инженерии», чтобы она принесла новым читателям такую же пользу. В то же время я хотел многое изменить, добавить информацию о недавних атаках и затронуть темы, которые в прошлом издании раскрыты не были.

И конечно же, я стремился сделать эту книгу намного лучше предыдущей: учесть советы фанатов, исследователей, читателей и авторов книжных обзоров. Так что сейчас кратко опишу, что именно вы найдете в этом издании, чего от него можно ожидать.

Согласно плану, намеченному в пирамиде, вторая глава («Видите ли вы то, что вижу я?») посвящена сбору данных из открытых источников. В

ней описаны техники, которые остаются актуальными независимо от времени. Я старался не слишком углубляться в описание специальных инструментов, хотя все же упомянул те, которые использовал на протяжении последнего десятилетия.

Третья глава («Профайлинг через общение») посвящена исследованию темы, которой в первом издании я касался весьма поверхностно. Теперь же продвинутое моделирование коммуникации и инструменты профайлинга мы обсудим намного подробнее.

В четвертой главе («Как стать кем угодно») мы погрузимся в изучение темы легендирования — то есть проникновения в систему жертвы под видом безвредного персонажа. За пределами мира социальной инженерии об этом говорят редко. Я же расскажу вам о некоторых уловках и приемах легендирования, а также приведу многочисленные личные примеры его применения — как успешного, так и провального.

В пятой главе («Я знаю, как тебе понравиться») я предоставил информацию об установке раппорта — то есть, попросту говоря, контакта, основанного на взаимопонимании. Эту информацию я набрал из огромного количества разных источников — подкастов, новостных рассылок и бесед с ведущими мировыми специалистами в этой области (например, с Робином Дрейке) — и описал ее в контексте социальной инженерии. Робин Дрейке — глава Отдела поведенческого анализа ФБР и по совместительству мой добрый друг. Этот человек по праву считается гуру в вопросах установки раппорта и доверия. И оба процесса он описал пошагово.

Шестая глава («Сила влияния») посвящена применению в социальной инженерии принципов, разработанных одним из ведущих исследователей темы влияния — Робертом Чалдини.

В седьмой главе («Оттачивая мастерство») мы обсудим фрейминг[10] и извлечение информации, а также разберемся, как освоить оба этих навыка.

В восьмой главе («Я знаю, о чем ты молчишь») мы обратимся к одной из моих любимых тем — невербальной коммуникации. Я подробно раскрыл ее в другой своей книге, «Разоблачение социальных инженеров: Человек в системе безопасности» (Unmasking the Social Engineer: The Human Element of Security; Wiley, 2014), а в этом издании составил своеобразный путеводитель для новичка.

В девятой главе («Взлом сознания») я покажу, как знания, описанные в моей книге, применяются на практике в разных типах СИ-атак. Из этой главы станет понятно, как важно социальным инженерам применять принципы, о которых я говорю.

Предпоследняя, десятая глава («Есть ли у вас ПЛАН?») посвящена предотвращению атак и минимизации их последствий. Ведь в книге о профессиональной социальной инженерии нельзя умолчать о четырех

основных шагах, которые необходимо пройти самим заказчикам СИ-проверок, чтобы научиться эффективно отражать атаки злоумышленников.

Но, как и все хорошее в этой жизни, книга должна закончиться. Основные выводы вы найдете в последней, одиннадцатой главе под названием «Что теперь?».

Как автор этой книги я могу вам пообещать следующее:

- Я обещаю не ссылаться на Wikipedia как на надежный источник, особенно когда речь идет об исследованиях (да, я учусь на своих ошибках).
- Я обещаю рассказать множество увлекательных историй, которые произошли со мной за последние семь с лишним лет. В некоторых случаях я буду даже разбирать эти случаи с разных сторон, чтобы вы увидели все важные нюансы. И не переживайте, я отберу разнообразные истории, так что скучно не будет.
- Рассказывая об исследованиях или работах специалистов из разных областей, я обязательно буду ссылаться на источники, чтобы вы сами смогли подробно изучить любую заинтересовавшую вас тему.

Как и после публикации моей первой книги, я буду рад услышать от вас комментарии, предложения и критику. А взамен прошу вас лишь воспринять эту книгу такой, какой она задумывалась. Если в мире социальной инженерии вы новичок, она поможет вам понять, как стать профессионалом. Если вы опытный специалист, хочется верить, что вас заинтересуют описанные примеры, советы и трюки (возможно, мне удастся даже чем-то обогатить ваш профессиональный арсенал). Если вы просто интересующийся энтузиаст, надеюсь, чтение этой книги принесет вам столько же удовольствия, сколько получил я, пока писал ее. Если же вы изначально настроены скептически, хочу отметить, что не считаю себя единственным и неповторимым пророком социальной инженерии. Я всего лишь специалист, который страстно любит свое дело, много лет занимается им и хочет поделиться накопленным опытом, чтобы мир, в котором мы живем, стал безопаснее.

Резюме

Ни одна из моих книг не была бы полной без кулинарных аналогий. Вот и сейчас не могу удержаться, чтобы не обратиться к этой теме. Итак, для приготовления вкусного блюда нужно четкое планирование, выверенный рецепт, свежие качественные продукты. А еще нужен одновременно научный и творческий подход к процессу приготовления. И здесь все будет решать мастерство повара. Социальная инженерия по природе своей штука довольно простая, но все же этот «рецепт» не для новичков. Социальный инженер должен понимать, как люди принимают решения,

что их мотивирует. Он должен знать, как контролировать собственные эмоции, манипулируя при этом чужими.

Тема этой книги сегодня не менее актуальна, чем восемь лет назад, возможно, она даже стала еще важнее. За эти годы мне довелось наблюдать за профессиональным становлением многих молодых социальных инженеров, а также за взлетами и падениями мошенников и злоумышленников.

В последнее время очень многие атаки направлены именно на эксплуатацию «человеческого фактора», поэтому специалисты в сфере безопасности просто обязаны разбираться в социальной инженерии. Но и это лишь частный случай применения собранных в этой книге знаний. Помню, когда я только начинал работать поваром (кажется, это было в прошлой жизни), мой учитель советовал мне пробовать каждый ингредиент, который я собираюсь использовать. Зачем?

Он сказал, что я не смогу добиться нужного вкуса блюда, если не попробую по отдельности каждый из его элементов. То есть когда я увижу в рецепте хрен, то буду знать: если захочу сделать блюдо острее, то просто добавлю больше хрена. Или, зная, что один из ингредиентов соленый, я не должен солить блюдо. В общем, вы поняли.

Даже если вы не работаете в сфере безопасности, вам все равно важно понимать, каков «на вкус» каждый ингредиент манипуляции — так вы успешнее сможете себя защитить. Как возникает раппорт в общении и как его могут использовать преступники, чтобы вытянуть у вас деньги? (Смотрите пятую главу.) Каким образом влияние, оказанное на собеседника в ходе телефонного разговора, заставляет его назвать пароль к своему аккаунту? (Подробности в главах шесть и семь.)

Каждый ингредиент важен и поможет понять вкус «блюда» под названием «социальная инженерия». Изучив все приемы по отдельности, вы научитесь видеть, что кто-то пытается применить их и повлиять на вас. И тогда вы успеете защититься.

Смотрели когда-нибудь кулинарные шоу Гордона Рамзи? Он всегда ясно формулирует, что именно ему не нравится в блюде. Например: «Здесь слишком много перца и масла». А новичок, возможно, сказал бы: «Блюдо слишком острое и жирное». Существенно ли отличаются эти формулировки? По-моему, да. И я хочу помочь вам стать Гордонами Рамзи мира социальной инженерии (но, конечно, не такими сквернословами).

Итак, приступим же к делу. И начнем с обсуждения сбора данных из открытых источников.

2 Видите ли вы то, что вижу я?

Помните, что неудача — это лишь событие, которое не делает человека неудачником.

Зиг Зиглар

Сбор данных в открытых источниках — фундамент деятельности социального инженера. С обработки информации начинается и на использовании информации держится любая операция. Именно поэтому нужно разобраться, какие способы получения информации об объектах воздействия доступны социальным инженерам.

Вне зависимости от того, какой способ использования открытых источников вы выберете, важно заранее четко знать, что именно вы ищете. А это не так просто, как кажется. Ведь формулировка в духе «Хочу найти всю доступную информацию об объекте» — это не цель. Разная информация имеет для нас разную ценность, и ценность эта варьируется в зависимости от выбранного типа атаки.

Сбор данных из открытых источников в реальной практике

Давайте для начала я помогу вам увидеть ситуацию в целом. Согласно данным с сайта http://www.worldwidewebsize.com, на сегодняшний момент в мире зарегистрировано больше 4,48 млрд веб-страниц. Причем сюда не входят неиндексированные страницы, теневой интернет и т.п. Ежегодный мировой интернет-трафик достиг 1,3 зеттабайт (то есть 1 300 000 000 000 000 000 000 байт). В общей сложности в интернете может храниться порядка 10 йоттабайт данных (в байтах это 10 000 000 000 000 000 000 000 000).

ЗАБАВНЫЙ ФАКТ

Йоттабайт, как ни странно, следующий за зеттабайтом, был назван в честь персонажа «Звездных войн» — магистра Йоды. Впрочем, существуют несколько других категорий для еще бóльших чисел и с еще более странными именами: например, shilentno-байт и domegemegrotte-байт.

Почему так важно представлять себе объем интернет-трафика? Например, если вы планируете адресный фишинг, вам необходимо искать информацию о хобби, предпочтениях и ценностях жертвы. Если же вы готовитесь к вишингу, больше смысла будет в сборе информации о месте работы жертвы и ее статусе в своей организации. Также стоит узнать обо всех внешних и внутренних службах, звонку из которых этот человек не будет удивлен. Если же вы собираетесь общаться с объектом воздействия лично, вам нужно знать, в каких местах и с какими людьми он обычно встречается.

Так вот, искать эти данные придется среди 4,48 млрд сайтов. Так что прежде чем погружаться в эту бездну, имеет смысл составить план поисковых работ.

Список вопросов, собранных в таблице 2.1 поможет вам выделить ключевые параметры поиска.

Конечно, вопросы из этой таблицы не предусматривают всего на свете. Но вы можете вносить в нее собственные дополнения: о типах используемых компьютеров, расписаниях сотрудников, употребляемых языках, антивирусных программах и пр.

Таблица 2.1. Вопросы для сбора данных из открытых источников

Тип организации	Какие вопросы задать себе
Корпорация/ компания	Каким образом организован доступ в интернет? Каким образом организован доступ в социальные сети? Есть ли у компании особые требования к тому, что сотрудники могут или не могут публиковать в Сети? Сколько у компании подрядчиков? Что это за подрядчики? Каким образом компания принимает платежи? Каким образом компания оформляет собственные платежи? Есть ли у нее свои колл-центры? Где находится головной офис, колл-центры или другие подразделения компании? Разрешено ли сотрудникам использовать собственные устройства на рабочем месте (BYOD)? Находится ли компания в одном месте или же имеет представительства в разных? Можно ли получить доступ к штатному расписанию?
Отдельный человек	Есть ли у него аккаунты в социальных сетях? Какие у него хобби? Куда он ездит в отпуск? Есть ли у него любимые рестораны? Особенности его семейной истории (наследственные болезни, семейный бизнес и т. п.). Какое у человека образование? Чему он учился? Какая у человека роль на работе (в том числе работает ли он из дома, на себя или на кого-то, перед кем отчитывается)? Упоминается ли имя человека на каких-либо сайтах (возможно, он где-то выступал, принимал участие в форумах или являлся членом клуба)? Владеет ли он недвижимостью? Если да, то какие платит налоги, выплачивает ли ипотеку и т. п.? Как зовут членов его семьи? (О каждом из них можно задать все приведенные выше вопросы.)

А вот реальная история, попавшая в новости в 2017 году (подробности здесь: https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitteraccount-1793843641). Ее герой — бывший директор ФБР Джеймс Коми. Одна блогерша решила проверить, удастся ли найти аккаунты Коми в социальных сетях. Поскольку он занимал высокую должность, эту информацию нигде особенно не светили. В таких ситуациях и

используется сбор данных из открытых источников. На илл. 2.1 представлена пошаговая последовательность действий, которые предприняла блогерша. Изучите ее, а я пока разберу каждый шаг по отдельности.

Во-первых, девушка четко сформулировала свою цель: выяснить, использовал ли глава ФБР социальные сети и если да — то какие.

Интернет эту задачу не облегчил: в 2016 году был опубликован рейтинг «Топ-60 соцсетей» — поле для поиска было огромным. Причем на каждой из этих платформ действовали свои правила и методы работы. Одному человеку было бы слишком сложно обработать такой объем информации.

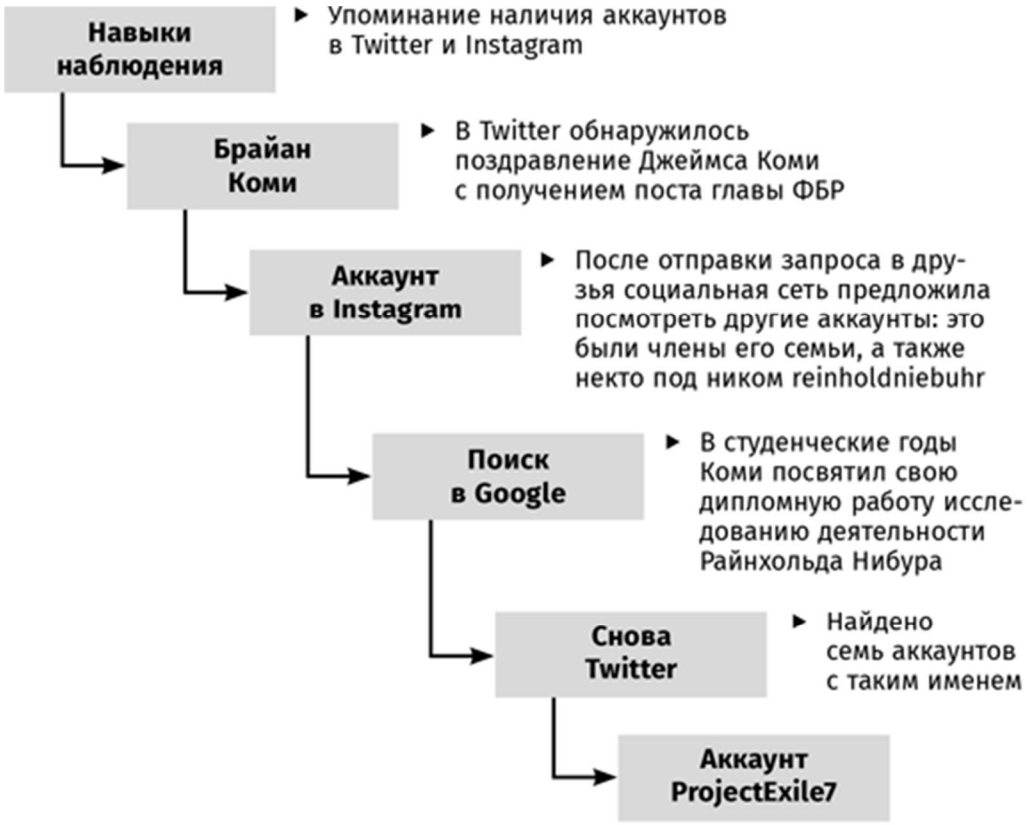
К счастью, одна из самых старых форм сбора данных из открытых источников довольно проста в применении: иногда оказывается достаточным просто внимательно слушать. В одном из интервью Коми упомянул, что у него были аккаунты в Twitter и Instagram.

Это позволило девушке существенно сузить поле поиска: с 60 соцсетей до двух. Согласитесь, задача значительно упростилась.

Аккаунтов, принадлежащих Джеймсу Коми, девушка не нашла, однако обнаружила в Twitter аккаунт его сына, Брайана Коми. Родственную связь между ними удалось подтвердить, когда Брайан поздравил Джеймса с повышением до должности директора ФБР.

Многие пользователи связывают между собой аккаунты в разных социальных сетях. Так поступил и Брайан: связал странички в Instagram и Twitter. Но аккаунт в Instagram оказался закрытым, и получить доступ к публикациям можно было только с разрешения самого Брайана.

Блогерша направила Брайану запрос на подписку. А в Instagram есть специальные алгоритмы, которые на основе отправленного запроса рекомендуют и других, потенциально интересных вам пользователей. Так вот, социальная сеть вывела несколько профилей членов семьи Брайана (Джеймса Коми среди них не было) и один аккаунт с ником @reinholdniebuhr.



Илл. 2.1. Поразительно эффективный сбор данных из открытых источников об объекте, скрывающем свою личность в соцсетях

Поиск в Google показал, что Райнхольд Нибур — американский теолог, философ и политический аналитик. Умер он в 1971 году и завести себе аккаунт в Instagram не мог. Посвятив еще некоторое время поискам, девушка обнаружила, что дипломная работа Джеймса Коми была посвящена деятельности именно Райнхольда Нибура.

Вооружившись новыми знаниями, блогерша вернулась в Twitter и нашла семь аккаунтов с таким именем. Один из них использовал это имя и ник @ProjectExile7.

Дальнейший поиск занял совсем немного времени. Выяснилось, что, когда Коми занимал должность прокурора и жил в Ричмонде, он запустил одноименный проект — Project Exile («Исход»).

Для сбора этой информации девушка не использовала незаконных методов, ей не пришлось ничего взламывать, она просто изучила информацию из открытых источников, обращая внимание на то, что могло оказаться важным.

Перед нами отличный пример поиска информации в открытых источниках как с помощью технических достижений, так и без них. Есть чему поучиться социальным инженерам! При написании этой главы я старался придерживаться такого же подхода, поэтому сейчас мы будем обсуждать, как совмещать использование разных источников открытой информации. Весь материал я разделил на две части: поиск данных, связанный и не связанный с использованием технологий.

ВЕСТИ ДОКУМЕНТАЦИЮ ИЛИ НЕ ВЕСТИ — ВОТ В ЧЕМ ВОПРОС

Прежде чем мы погрузимся в изучение процесса поиска информации, я хочу взять небольшую паузу и изложить свои мысли по поводу документирования процесса и результатов деятельности социального инженера.

Вопрос даже не в том, нужно ли вести письменные отчеты. И так понятно, что делать это необходимо. Но что именно документировать и в каком объеме?

Вспомните, что я говорил в начале этой главы: продираясь через 10 йоттабайт собранных в Сети данных, вы узнаете об объектах воздействия очень многое. И если природа не наградила вас фотографической памятью, никакой уровень интеллекта не позволит вам запомнить все детали. На самом деле даже специалисты с фотографической памятью не смогут составить полноценный отчет о деятельности, полагаясь только на свои воспоминания.

Я не скажу, что конкретно вам нужно записывать, потому что в каждой ситуации задействовано слишком много различных факторов. Например, в начале своего профессионального пути в сфере СИ, работая в гордом одиночестве, я придумал особую систему использования блокнотов: она позволяла собирать по каждому клиенту отдельные папочки, в которые были сложены заметки. В каждой такой заметке я выделял несколько разделов: личную информацию, данные о компании, семье, активности в социальных сетях и т.п. Любой новый блок полезной информации, обнаруженный в процессе исследования открытых источников, я помещал в соответствующий раздел соответствующего документа. В результате писать финальные отчеты мне стало намного легче. Применял я и другие приемы: например, определенными цветами выделял информацию, которая могла пригодиться в ходе атаки. Один цвет — для данных, которые были просто полезны, другой — для информации, которая оказалась ключевой.

Когда у меня появилась своя команда и над проектами стали работать несколько человек одновременно, оказалось, что неудобно то и дело передавать друг другу бесчисленные блокноты. Тогда я нашел решение, позволявшее всей команде вести общие заметки.

Сначала мы использовали решения вроде Google-диска, я опробовал разнообразные облачные приложения и инструменты.

Однако все эти решения имели свои недостатки.

- Мне нужно было собирать номера социального страхования, банковские данные и другую приватную информацию о жизни объектов. И что бы я делал в случае взлома? (Например, в 2013 году взломали систему безопасности программы Evernote и 50 млн пользователей пришлось менять пароли.)

- Я не мог напрямую контролировать использование таких программ или управление хранящимися в них данными.
- Стоило мне упомянуть в общении с клиентами слово «облако», как многие из них тут же отвечали решительным «нет!».

Так я понял, что необходимо создать собственные серверы. Мы закупили место на проверенных и защищенных серверах. Создали собственный защищенный VPN-сервер и установили ПО, которое выбрали сами. Все это оградили стеной файерволов, роутеров и VPN.

Теперь я мог контролировать собранную информацию управлять ею, обновлять, передавать и обеспечивать ее максимальную защищенность. Короче говоря, по ночам можно было спать спокойно и не бояться, что данные моих клиентов кто-то похитит.

Возможно, вы найдете другое решение. Главное — относиться к хранению, управлению, обновлению, передаче и обеспечению собранных данных о клиентах с максимальной серьезностью.

Не связанные с использованием технологий методы сбора данных из открытых источников

Сюда я отношу любые действия социального инженера, не предполагающие использование компьютера. Вы можете подсмотреть, как компьютером пользуется ваш объект, но сами, как социальный инженер, к гаджетам притрагиваться не должны: информация собирается без использования техники. В этом разделе можно было бы описать огромное количество самых разных методов — для удобства назовем их навыками наблюдения. Ниже я объясню, что это такое, и приведу некоторые примеры.

Навыки наблюдения

На первый взгляд может показаться, что наблюдать очень просто. Тем не менее успешно использовать наблюдение в работе удается далеко не каждому, особенно сегодня, когда все стали зависимы от соцсетей. Да и маркетологи из кожи вон лезут, обучая нас не обращать внимания на детали. В 2015 году Эмили Драго из Университета Элон провела исследование под названием «Влияние технологий на личное общение». Его результаты показали, что развитие гаджетов связано со снижением качества общения в реальной жизни. 62% участников исследования пользовались мобильными телефонами во время живого общения, хотя прекрасно понимали, что это не помогает вести беседу.

ЗАМЕТКА Результаты исследования «Влияние технологий на личное общение» (на английском) можно найти на сайте

университета https://www.elon.edu/docs/e-web/academics/communications/research/vol6no1/02DragoEJSpring15.pdf.

Мы живем в век эмодзи, мемов, сообщений из 280 символов и постов в социальных сетях. Темпы развития технологий восхищают. Однако эти самые технологии и создали условия, в которых люди разучились наблюдать за собеседником. Поэтому мы и начали разбор темы сбора информации с методов, не предполагающих использование технологий.

Возможно, сейчас вы задаетесь вопросами:

- Что означает термин «навыки наблюдения»?
- Как эти навыки можно у себя развить?
- Что это даст?

Давайте обсудим каждый из них и посмотрим, что вам удастся заметить и понять.

Что включают в себя навыки наблюдения?

Ниже описаны несколько сценариев, отражающих применение навыков наблюдения в жизни.

Сценарий первый

Ваша задача — пробраться в канцелярию крупной медицинской клиники. Причем сделать это при свете дня. Взламывать замки, пробираться через заборы и влезать в окна нельзя. Нужно проверить, позволят ли вам сотрудники рецепции и охраны пройти в помещение с ограниченным доступом. Иными словами, надо проникнуть в клинику и попасть в те ее отделения, где позволено находиться только персоналу.

Вот какие данные вы можете собрать из открытых источников с помощью наблюдения:

- Одежда. Этому простому фактору обычно уделяют мало внимания, а зря. Еще в первой главе я говорил, что социальным инженерам нужно подтолкнуть объект воздействия к принятию необдуманных решений. Поэтому если при попытке проникнуть в здание, куда все сотрудники приходят в повседневной одежде, вы нарядитесь в костюм-тройку, то обязательно привлечете к себе всеобщее внимание. Так что нужно понимать, как будут одеты окружающие, и выглядеть соответствующе.
- Входы и выходы. Точки входа и выхода нужно найти заранее, до того как вы попадете на территорию объекта. Существует ли место для курения, через которое можно проникнуть в здание? Все ли входы охраняются одинаково? Когда охранники сдают смену, какие входы остаются без охраны или без должного внимания со стороны охраны?

- Организация прохода. Как организован проход на территорию и в здание? Есть ли у сотрудников бейджи и пропуска? Какие? Где их принято закреплять? Надо ли знать некий код? Существует ли порядок, при котором сторонних посетителей сопровождает по территории до места назначения охранник? Выдают ли им особые пропуска? Наконец, есть ли на запланированной точке входа в здание турникеты, пост охраны или другие препятствия?
- Охрана периметра. Узнайте, что обычно происходит снаружи здания. Установлены ли там камеры наблюдения? Обходят ли территорию охранники? Закрыты ли мусорные баки? Установлены ли системы сигнализации или датчики движения?
- Сотрудники охраны. Как они работают: расслабленно сидят, уставившись в экран телефона или компьютера, или же охранники всегда начеку и внимательно следят за происходящим? Как вы думаете, им на работе скучно или интересно?
- Организация пространства. Позволяет ли расположение пропускных систем подсмотреть пароль из-за плеча стоящего впереди человека? (Иными словами, можно ли подойти к сотрудникам компании настолько близко, чтобы рассмотреть, какой код они используют для входа?)

Конечно, есть еще огромное количество вещей, на которые надо обратить внимание, однако эти — основные.

Чтобы вы поняли, почему я выделяю именно их, расскажу одну реальную историю, в которой важнейшую роль сыграли одежда, входы и выходы, организация прохода на территорию и охрана периметра. Мы вместе с Мишель (впоследствии — моим техническим консультантом во время работы над этой книгой) должны были реализовать сценарий, который я описал в начале этого подраздела. Чтобы собрать необходимые данные из открытых источников, мы, конечно же, применяли технологические средства (о которых я подробнее расскажу позже). Но и нетехнической разведке уделили немало внимания.

В качестве предлога для вторжения мы выбрали легенду, согласно которой компанию по борьбе с паразитами якобы вызвали для уничтожения расплодившихся пауков. Свою «компанию» мы назвали Big Blue Pest Control и подобрали соответствующий реквизит: синюю униформу и бутылки с распылителем, которые наполнили «ядом» для пауков (на самом деле в баллонах был ярко-синий изотоник от Gatorade).

ЗАБАВНЫЙ ФАКТ Синий изотоник в бутылках вместо яда для насекомых — отличный способ пронести с собой на операцию освежающий напиток, который поможет утолить вызванную волнением жажду и не вспотеть. Но есть у такого решения и свои минусы: если кто-то увидит, как вы откручиваете с баллона распылитель и глотаете налитый в него яд, то как минимум вызовете у этого человека подозрение.

Для начала мы объехали периметр клиники, отметили все входы и выходы, расположение камер и места для курения. Обратили внимание, где собиралось больше и меньше людей. Мы отметили, как сотрудники носят бейджи и как одеваются. Затем выбрали подходящую, на наш взгляд, точку для проникновения и направились к двери. Нам нужно было собрать максимум информации о том, как именно организован проход на территорию.

Два охранника наблюдали за тем, как сотрудники прикладывали пропуска к металлическому автомату и проходили внутрь. Кроме того, справа была стойка охраны, за которой сидел ответственный за регистрацию посетителей сотрудник.

Мы решили пройти мимо охранников, слившись с толпой. Это не сработало: нас тут же остановили и спросили, чего мы хотим. Я прочел на бейдже ближайшего охранника его имя и сказал: «Здравствуйте, Эндрю. Нас попросили рассказать об услугах нашей компании по срочному уничтожению пауков…» Охранник прервал меня на полуслове: «Хорошо, зарегистрируйтесь на стойке».

Я было обрадовался, что дело сделано, но тут сотрудник за стойкой попросил назвать наши имена. Я выдумал что-то на ходу, но он порылся в своих бумагах и сказал: «К сожалению, вас нет в списке посетителей. Вход посторонних лиц без пропуска запрещен».

Мы пытались объяснять, просили о помощи и даже пробовали давить на него. Не сработало. Пришлось сворачиваться. Мы вышли через главный вход и решили еще разок обойти здание и заодно обсудить дальнейший план действий. И тут я заметил, как несколько человек вышли покурить. Я попросил Мишель подождать и подошел к курильщикам, при этом держал себя так, слово занят важным делом: осматриваю территорию и делаю пометки в блокноте.

Затем мы медленно продолжили обход, пока не заметили группу людей, направлявшихся к другой двери, — и увязались за ними. За дверью начинался коридор, но оказалось, что он вел к тому же пропускному пункту, где нас только что развернули. Тут я увидел справа от себя лифт — но без кнопки вызова. «Черт побери, видимо, им управляют с поста охраны», — только и успел подумать я, как двери лифта распахнулись. Я тут же шагнул внутрь, надеясь, что Мишель это заметит и последует за мной.

К счастью, она в подобных ситуациях чувствует себя как рыба в воде, не теряется и не волнуется. В лифте уже ехала группа людей. Громко, чтобы все это услышали, Мишель принялась канючить, обращаясь ко мне, как к начальнику: «А мы скоро закончим? Я просто умираю с голоду, а вы говорили, что никакого обеда не будет, пока все не доделаем».

Одна из попутчиц строго взглянула на меня и сказала:

— Дали бы человеку поесть!

На что я ответил:

— Я бы с удовольствием, но нам осталось проверить еще один этаж. И чем раньше мы это сделаем, тем быстрее пойдем на обед.

Женщина вздохнула и спросила:

— Так на какой вам этаж?

— Нам в канцелярию, — уверенно ответил я.

Женщина достала свой пропуск, провела им по индикатору, после чего нажала какую-то комбинацию кнопок на экране и сказала:

— Сейчас мы вас там и высадим.

Уф! Нам повезло: благодаря невероятной наблюдательности Мишель и моему умению быстро реагировать мы не только не попались охране, но еще получили в невольные помощники сотрудницу и прошли по ее пропуску на охраняемый этаж (кстати говоря, Мишель не сильно лукавила, ведь она всегда голодная).

Мы вышли из лифта на этаже, где располагалась канцелярия, и уткнулись в закрытую дверь с табличкой, гласившей: «Если вам нужна помощь, позвоните». Что ж, мы позвонили.

Нам ответила женщина:

— Чем могу помочь?

Мы повторили свою историю о презентации, на что она сказала:

— Хорошо, я только позвоню на охрану и получу от них добро.

Если бы она это сделала, нас, конечно же, вышвырнули бы вон, поэтому я сказал:

— Звоните, если хотите. Но вообще-то нас Эндрю сюда послал.

— А, Эндрю? Тогда проходите.

Женщина открыла дверь и добавила:

— Только письма не трогайте, пожалуйста.

Мы спокойно перелопатили все помещение: сдвигали потолочную плитку и стопки писем, ковырялись в проводах. Как видите, случившееся во многом было завязано на наблюдательности и умении сортировать найденную информацию (причем это было только самое начало операции).

Я понятия не имел, пригодится ли мне имя Эндрю. Мишель не могла заранее знать, что в лифте нам попадется сердобольная сотрудница. И никто из нас не предполагал встретить группу курильщиков, которым будет совершенно все равно, что мы вошли в здание вслед за ними. Однако благодаря наблюдательности все эти мелочи обеспечили нам необходимые для успеха операции условия.

Сценарий второй

Как вам такая задача: провести адресный фишинг топовой юристки из крупной американской юридической корпорации? Условие: для подготовки операции можно использовать только информацию из открытых источников.

Мы разберем эту историю подробнее в разделе, посвященном сбору информации с использованием технологий. Тем не менее сейчас мне хочется поделиться историей своего провала в задании, а также важными уроками, которые я из этого провала извлек.

Выполняя задачу, мы выяснили, что юристка среди прочего вела некоторые дела в штате Массачусетс. Именно там незадолго до описанных событий изменилось налоговое законодательство. Я подумал, что эта новость наверняка привлечет ее внимание и заставит открыть приложенный к письму файл.

Я начал составлять письмо об изменениях законов штата и подробнейшим образом планировать все этапы операции. Письмо было написано профессионально, в нем не прослеживалось даже намека на какую-либо угрозу, зато был огромный соблазн открыть зараженный файл. Дело в том, что в письме был сформулирован реалистичный срок для прочтения и формулировки ответа, к тому же оно было подробным ровно в той степени, чтобы получателю захотелось нажать на ссылку, обещавшую продолжение.

Увы, через считаные минуты после отправки письма наш план раскусили и операция провалилась. Вы догадались, где была допущена ошибка?

Массачусетс юридически является не штатом, а содружеством. Юристка, по долгу службы обращавшая внимание на детали, получила письмо об изменениях в налоговом законодательстве штата Массачусетс и сказала себе: «Хм, ведь они должны знать, что это никакой не штат!» Затем она присмотрелась к адресу отправителя и ссылке на документ — это вызвало у нее достаточно подозрений, чтобы пожаловаться на спам. Афера не удалась.

Мы же со своей стороны не обратили внимания на эту «мелочь», и отсутствие наблюдательности в данном случае обошлось нам дорого.

Вывод? Наблюдательность нужно сохранять всегда, несущественных деталей не бывает. Рассуждайте как человек, на которого вы пытаетесь оказать влияние. Старайтесь понять, чего он ждет, и оправдывайте его ожидания. А иначе дьявол, скрытый в деталях, вас же и погубит.

Как освоить эти навыки?

Эту тему сложно уместить в короткую книжную главу. У каждого человека есть индивидуальный набор врожденных и приобретенных способностей, которые могут как усложнять, так и облегчать процесс

освоения навыков. И поскольку мы с вами не знакомы лично, единственное, что я могу сделать, — это рассказать о собственном методе.

Его можно сравнить с игрой в «Захват флага». Попадая в новое здание (например, в стоматологическую клинику), я говорю себе: «Мне нужно будет запомнить двух первых человек, которых я увижу: цвет их одежды, что они делают».

Кроме того, я сам для себя выставляю ограничивающие условия:

- Эти люди не должны быть представителями обслуживающего персонала за стойкой.
- Нельзя забывать об основной задаче или отклоняться от нее.
- Никаких записей!

Итак, находясь в здании, я наблюдаю и стараюсь сохранить в памяти максимум подробностей до тех пор, пока не выхожу на улицу. Получается что-то вроде:

- Пожилая женщина сидела слева в голубой кофте и читала журнал Woman's Day.
- Мальчик в полосатой футболке раскладывал на полу кубики.

Я делаю в уме такие заметки и изо всех сил стараюсь их запомнить. Для этого я использую разные мнемонические приемы: например, несколько раз повторяю информацию, пытаясь впечатать ее в память.

Как только я осваиваю навык составления таких ментальных заметок без дополнительных усилий, я усложняю задачу. В конце концов мои «флаги» выглядят примерно так:

- Какого пола были люди.
- Что на них надето.
- Чем они занимались, когда я их увидел.
- Предполагаемый коммуникативный профиль каждого (подробнее мы поговорим об этом в третьей главе).
- Что сообщал язык их тела.
- На основе этих данных формулирую в уме некую историю о том, почему они оказались в том месте, где я их застал. С помощью этой истории я и запоминаю необходимую информацию.

Честно говоря, этот метод давал шикарные результаты. Даже с моей ужасной памятью я умудрялся вспомнить офис, в который заходил три-четыре года назад и где встретил двух женщин в черных юбках и белых рубашках на пуговицах, что-то читавших со своих iPad. Одной из них была явно не по душе ее соседка (ну или же ей просто нужно было куда-то уйти). Я пришел к такому выводу, потому что, хотя женщины и сидели

рядом, тело той, что слева, было направлено в противоположную сторону.

Еще за стойкой стоял мужчина в форме охранника: помню его черный костюм, белую рубашку, черный галстук. На правом запястье он носил золотые часы, из чего я сделал вывод, что он левша. Его волосы были аккуратно уложены, борода подстрижена. Он внимательно следил за мной и за всеми, кто находился в холле, и делал в блокноте пометки от руки.

У стойки на стуле сидел молодой мужчина с газетой в руках. Но мне показалось, что он только притворялся читающим, а сам смотрел в одно место и края газеты при этом тряслись. Я придумал историю о том, что он пришел на собеседование, конечно же, нервничал и безуспешно пытался отвлечься чтением.

Сейчас, когда я пишу эти строки, то представляю это помещение абсолютно четко, словно нахожусь в нем. Маленькие наблюдения способны сослужить вам, как социальному инженеру, огромную службу. Кроме того, я рекомендую отслеживать ваши слабые стороны и развивать их, начиная с малого. Проникнитесь этой мыслью: без практики в нашем деле никуда. Слишком часто мне встречаются люди, которые хотят достичь всего и сразу. Однако для формирования любого навыка требуется время.

Неудачи могут научить нас даже большему, чем успехи, — если позволить себе учиться, конечно. Именно поэтому я должен отдельно поговорить про ожидания.

Каких ожидать результатов?

В книге «Разоблачение социальных инженеров», которую мы написали вместе с доктором наук Полом Экманом, я сосредоточился исключительно на невербальных сигналах: языке тела и мимике. Когда я только учился замечать, различать и интерпретировать их, то казался себе супергероем, способным читать мысли. Я смотрел собеседнику в лицо и видел эмоции, которые тот старался скрыть. Затем сопоставлял их с языком тела и другими действиями, так что в результате практически предсказывал его реакцию на различные вопросы и ситуации. И что самое удивительное: мои предсказания оказывались верными больше чем в половине случаев. Но потом начались проблемы. Да, почти в 75% ситуаций я оказывался прав — но это ведь значит, что в оставшихся 25% я ошибался. Кроме того, из-за этого ощущения всемогущества я переоценивал свои истинные способности в роли социального инженера. Мне казалось, что я вижу и понимаю больше, чем видел и понимал на самом деле.

Работа с Экманом стала для меня своеобразным уроком смирения: Пол постоянно находил в моих интерпретациях ошибки и исправлял их.

Однажды он сказал: «Крис, даже если ты знаешь, что человек ощущает, ты не всегда можешь верно понять, почему это с ним происходит».

И, прежде чем мы перейдем к обсуждению ожиданий, я хочу, чтобы вы запомнили: даже если вы застали человека за каким-то действием, это не означает, что вы автоматически поймете причины его поступка. Так как же найти связь между этими «что» и «почему»? Есть несколько способов: с помощью вопросов, сбора дополнительной информации и дальнейшего наблюдения.

Однажды во время занятия я рассказывал историю из своей СИ-практики и вдруг заметил на лице одного из слушателей откровенно злое выражение. Язык его тела показывал, что он закрылся: сложил руки на груди, откинулся на спинку стула и вытянул ноги. Я подумал, что мои слова вызывали у него недоверие, и начал уделять ему больше внимания, но это не спасло положения: мужчина только больше отстранялся, а через несколько минут вдруг резко встал и вышел из аудитории.

Я недоумевал: в чем проблема? Ведь я все делал правильно, почему он злится на меня?

Во время перерыва я направился в туалет, погруженный в размышления об этой ситуации, и вдруг тот самый молодой человек подошел ко мне и сказал: «Извините, что мне пришлось выйти во время вашего выступления. Мне пришло сообщение от начальника о том, что на работе проблемы. Я пытался ему объяснить, что нахожусь на учебе, но он настоял, чтобы я взял трубку и ответил на его дурацкие вопросы. Подскажите, пожалуйста, как мне нагнать упущенное?»

Я не удержался и рассмеялся, а потом объяснил свою реакцию: рассказал, как интерпретировал увиденное. А в это самое время у меня в голове звучал голос доктора Экмана: «Крис, ну что я вам говорил?» Данная ситуация послужила мне отличным уроком по выявлению причинно-следственных связей.

Это правило относится и к наблюдению, и к сбору информации в открытых источниках. Не стоит думать, будто примеры, которые я привожу в этой книге, все сплошь иллюстрируют человеческую глупость. Я склоняюсь к тому, что люди просто недостаточно информированы о потенциальных опасностях, но никак не глупы.

Взгляните на илл. 2.2, сделайте в уме необходимые заметки. Рассуждайте как социальный инженер: что эта машина может сообщить вам о своем водителе? На илл. 2.3 один из элементов снимка увеличен для наглядности.

Справа приклеен символ поддержки больных раком груди. Слева — наклейка фонда помощи детям, оказавшимся в опасных для жизни ситуациях, Kids Wish Network. И еще одна говорящая наклейка, «10–20-пожизненно». Я не понимал ее смысла, но ответ быстро нашелся в

интернете: это слоган движения за более строгие судебные приговоры людям, совершившим преступление с использованием огнестрельного оружия.

Илл. 2.2. Что вы здесь видите?

Илл. 2.3. Так проще рассмотреть?

Что все эти наклейки говорят о водителе? Этот человек поддерживает благотворительные организации, деятельность которых считает важной. Возможно, член его семьи болел раком или столкнулся с детскими болезнями. Кроме того, водитель явно неравнодушен к вопросам контроля за огнестрельным оружием. Может, он сам был жертвой преступления с его использованием или лично знал людей, попавших в такую ситуацию.

Как думаете, готовы ли вы завести с водителем беседу теперь, когда собрали всю эту информацию?

Я призываю вас быть осторожнее с выводами. Обычно мои ученики отвечают: «Я заговорю с ним о том, почему наши законы в отношении огнестрельного оружия несовершенны» — или еще что-то в этом роде. Но для начала просто поставьте себя на место этого водителя и подумайте: возможно ли просто в ходе случайной беседы заставить вас изменить свою точку зрения? Вряд ли. Помните и о вашей

цели: сделать так, чтобы собеседник при общении с вами действовал, не думая. Для этого говорить нужно о том, что интересно ему, а не вам. Подробнее мы коснемся этой темы в седьмой главе, посвященной извлечению информации.

Илл. 2.4. Что вы можете сказать, глядя на эту фотографию?

Что вы видите? Какие выводы можете сделать как социальный инженер? Старайтесь обратить внимание на мельчайшие детали:

- Видно, что это за рабочая среда (офис).
- Понятно, какая операционная система установлена на компьютере.
- Видно, какой у человека планшет.
- Можно также сделать вывод, что он увлекается определенным сериалом.
- Видите, какой браузер и почтовый ящик использует этот человек?
- Какие еще признаки могут что-то сообщить о нем?
- Какие еще детали вы заметили?

Это всего лишь поверхностные заметки, опытному СИ-специалисту подобная фотография даст намного больше информации. Как думаете, можно ли на ее основе провести профайлинг, достаточный для составления пары фишинговых e-mail, которые вызвали бы у хозяина стола эмоциональную реакцию?

Впрочем, фотографии и даже личного общения не всегда бывает достаточно. В таких случаях на помощь социальному инженеру приходят технологии.

Сбор данных из открытых источников с использованием технологий

Прежде чем вы начнете писать негативный отзыв на эту книгу и жаловаться, что я не предоставил исчерпывающий список инструментов для сбора данных, позвольте мне сказать вот что:

Действительно, в этой главе НЕ будет полного списка инструментов, процессов и методов сбора информации из открытых источников с использованием технологических средств.

Но вот что здесь будет. В этой части главы мы обсудим инструменты и техники, которые я сам использую в работе каждый день. А копнуть глубже вам помогут другие известные специалисты в этой области. Вот лишь пара имен людей, с которыми мне довелось общаться лично:

- Ник Ферно. Я специально слетал в Великобританию на его четырехдневный курс, от которого остался в полном восторге. Он открыл мне глаза на то, какие махинации можно провернуть с API (программными интерфейсами приложений) и как на самом деле работают приложения соцсетей. Вот сайт Ника: https://www.csitech.co.uk/.
- Майк Баззелл. Майк — человек, к которому нужно обращаться, когда необходимо исчезнуть с просторов Всемирной сети. Кроме того, он разработал удивительные инструменты для поиска информации в открытых источниках: социальных сетях и с помощью поисковых систем. Адрес его сайта: https://inteltechniques.com/.

Эти славные парни — мои добрые друзья. Я учился у них, не раз спрашивал совета и просил помощи. Честно признаюсь: я считаю их настоящими мастерами сбора данных из открытых источников. (Бесстыдное хвастовство: они оба выступали в СИ-подкасте. Ищите подробности по запросу «OSINT».)

Я же сейчас сосредоточусь на вещах, которые использую в своей работе ежедневно. Их можно разделить на четыре «вида»: соцсети, поисковые системы, Google и другие инструменты. О каждом из них мы поговорим отдельно. Я хочу сформировать у вас общее представление о том, что делаю я, а вы уже сами решите, что нужно изучить подробно лично вам.

Социальные сети

Нельзя писать про поиск информации в открытых источниках и хотя бы вскользь не упомянуть социальные сети. Честно говоря, это очень странно: ведь я еще помню время, когда можно было получить по шапке за то, что заглянул в дневник сестры. Теперь же дневники не просто перекочевали в онлайн: личные записи можно читать, комментировать, лайкать.

Социальные сети стали неотъемлемой частью жизни.

Компания We Are Social собрала статистику, которая поможет составить представление о том, насколько велика эта часть (https://wearesocial.com/special-reports/digital-in-2017-globaloverview). На январь 2017-го:

- Население мира составляло 7,467 млрд человек.
- Из них интернетом пользовались 3,773 млрд.
- 2,789 млрд человек активно использовали социальные сети.
- Было зарегистрировано 4,917 млрд уникальных пользователей мобильных телефонов.
- 2,549 млрд человек подключались к соцсетям со смартфонов.

Эта информация крайне важна для социального инженера. Давайте рассмотрим функционал самых популярных платформ.

LinkedIn: более 106 млн пользователей. Здесь собрана следующая информация:

- ваша трудовая история;
- данные о вашем образовании;
- в какой школе вы учились;
- в каких клубах состояли и какие академические вершины покорили;
- какие люди способны подтвердить наличие у вас описанных навыков.

Facebook: 1,8 млрд пользователей. Здесь можно узнать о пользователе следующее:

- его любимая музыка;
- его любимые фильмы;
- в каких сообществах по интересам он состоит;
- с кем дружит;
- кто его родственники;
- куда ездил в отпуск;
- что любит есть;
- где жил;
- и многое, многое другое.

Twitter: 317 млн пользователей. Позволяет узнать:

- чем пользователь занят прямо сейчас;
- какие у него пищевые привычки;
- его геолокацию;
- эмоциональное состояние (правда, только в пределах 280 символов).

Можно было бы продолжить этот список, но, думаю, вы поняли, к чему я клоню. Даже эти три социальные сети позволяют собрать огромное

количество информации об объектах воздействия. И я осмелюсь заявить, что на ее основе нередко можно осуществить полноценный профайлинг.

ЗАБАВНЫЙ ФАКТ

В 87-м эпизоде СИ-подкаста мы разговаривали с профессором Джеймсом Пеннебейкером. Он создал инструмент (http://www.analyzewords.com/), анализирующий содержание аккаунта в Twitter на основе языка, которым пользуется его владелец. Мы загрузили в сервис аккаунт Мишель (@SultryAsian), и программа охарактеризовала ее как экстравагантную калифорнийку, позитивно настроенную и живущую настоящим моментом. Честно говоря, я тогда чуть не подавился: это описание — полная противоположность реальной Мишель… и точная характеристика образа, который она стремилась создать в соцсетях.

Не стоит путать оценку человека по социальным сетям и составление его реального психологического профиля. По врезке с «Забавным фактом» видно, что некоторые люди совершенно по-разному общаются в реальной и виртуальной жизни. И тем не менее социальные сети можно считать ценным источником информации для социального инженера, ведь многие атаки связаны как раз таки с «онлайн эго» человека. Найдите подход к виртуальному альтер эго объекта воздействия, и перед вами откроются новые векторы атаки.

Сегодня существуют сотни социальных сетей, которыми пользуются миллиарды людей. Для социальных инженеров это, конечно же, несметные богатства данных. Один из лучших способов сбора информации здесь дают поисковые системы, которые мы обсудим ниже.

Поисковые системы

Интернет постоянно меняется. Появляются новые, более удобные способы поиска нужной информации среди йоттабайт данных. Пользователям это безостановочное совершенствование только на руку, а вот социальным инженерам оно может помешать: ведь поисковики, которые работают сегодня, завтра могут уйти в небытие.

Помню, как появился Spokeo, источник отличной информации. Я пользовался им почти каждый день. Но чем популярнее он становился, тем больше в нем появлялось рекламы. Потом разработчики стали просить деньги за информацию, а результаты поиска все чаще оказывались ненадежными.

Наверное, излишне говорить, что сегодня использовать Spokeo бессмысленно. Я профессиональный социальный инженер, а значит, мое время стоит дорого. И если мне придется перепроверять каждый найденный с помощью какого-либо сервиса факт, я попросту лишусь работы.

Опубликовав свою первую и многие последующие книги, я понял, что читателям не нужны списки используемых мной инструментов. Часто происходило следующее:

- Когда книгу издавали, описанные инструменты и идеи их использования уже устаревали.
- Появлялись новые, более эффективные инструменты.
- Случалось и то и другое.

Так что в этот раз я решил отказаться от перечисления конкретных сайтов и инструментов. Вместо этого просто проведу вас через процесс сбора данных из открытых источников. Конечно, я укажу, какие средства использовал, но сосредоточусь в первую очередь на специфике их применения с точки зрения социальной инженерии.

Объектом стал мой добрый друг Ник Ферно (надеюсь, мы останемся друзьями и после выхода этой книги). Хочу обратить ваше внимание: я ничего плохого в отношении Ника не замышляю и отношусь к нему как к человеку сознательному и прекрасно разбирающемуся в вопросах безопасности. Но интернет хранит тайны каждого из нас, даже Ника. Нужно просто уметь правильно формулировать запрос.

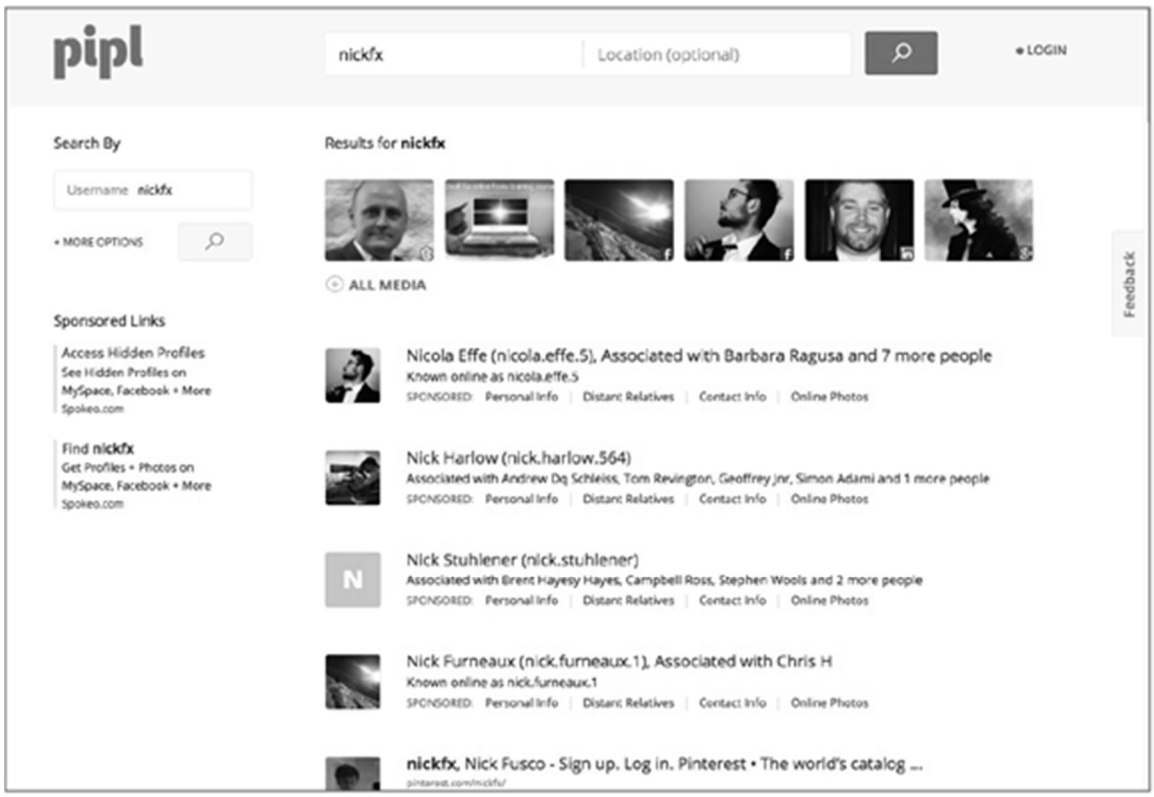
д0ксинг Ферно

д0ксинг — это что за зверь? На хакерском сленге «доксить» — значит собирать конфиденциальную информацию о личной жизни объекта будущего воздействия. Эти данные обычно используют в процессе атаки, для компрометирования и унижения жертвы или совершения иных запрещенных действий.

Ни одну из этих целей я, конечно, не преследовал, а просто хочу продемонстрировать вам потенциал открытых источников и возможности использования полученной информации. Обычно я начинаю сбор нужных мне данных об объекте с обращения к сервису https://pipl.com/.

Pipl похож на смесь ресурса White Pages и социальных сетей. Этот сайт хорош тем, что позволяет искать людей по реальному имени, имени пользователя и другим критериям.

Беглый поиск показывает, что Ник зарегистрирован в Twitter как @nickfx. Давайте посмотрим, что найдется на https://pipl.com/ по этому имени пользователя (см. илл. 2.5).

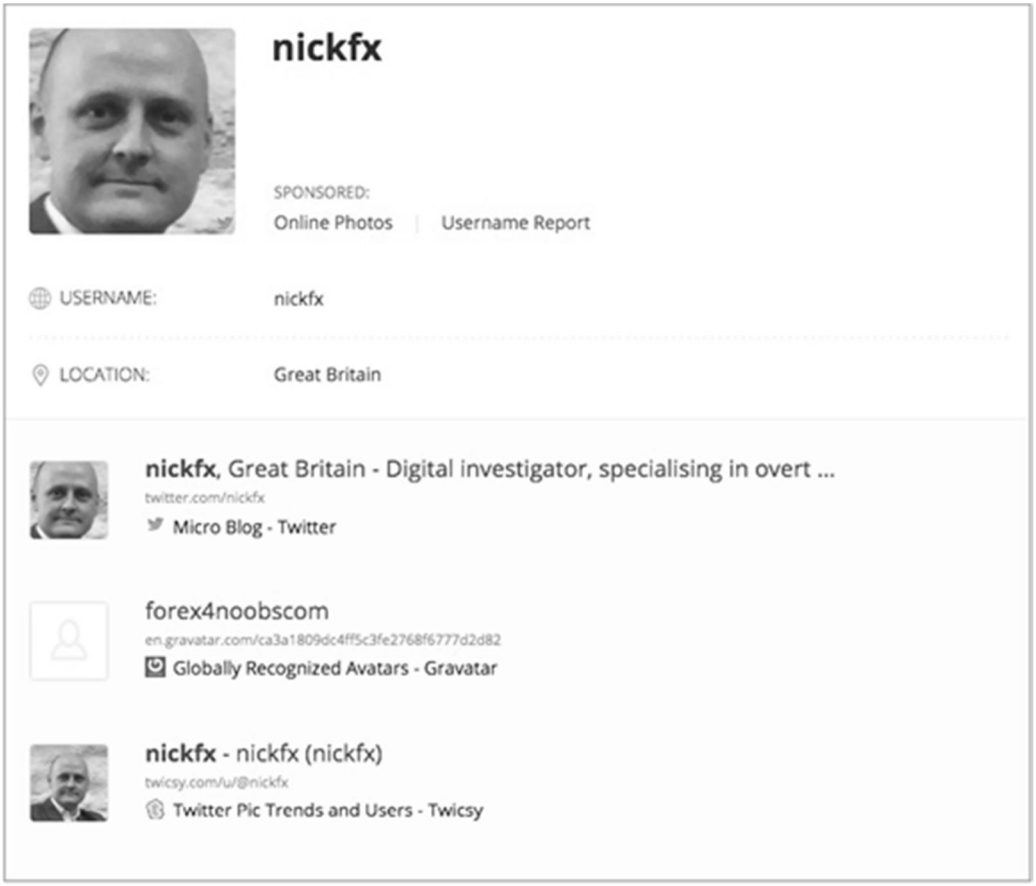


Илл. 2.5. Видите его?

При взгляде на экран сразу становится понятно, что на первой же фотографии изображен нужный нам «Ник», а чуть ниже указан некий Ник Ферно, связанный с Крисом Х (кто бы это мог быть?), но имя пользователя уже другое.

Прежде чем двинуться дальше, предлагаю проверить, что произойдет, если я нажму на фотографию Ника (см. илл. 2.6).

Произошло то, что мы и предполагали: это тот человек, который нам нужен. Кроме того… мы видим его геолокацию! Не устаю восхищаться возможностями открытых источников! Посмотрите на илл. 2.7.



Илл. 2.6. Подтверждение

Илл. 2.7. Еще больше данных!

```
User-agent: *
Crawl-delay: 10
# CSS, JS, Images
Allow: /misc/*.css$
Allow: /misc/*.css?
Allow: /misc/*.js$
Allow: /misc/*.js?
Allow: /misc/*.gif
Allow: /misc/*.jpg
Allow: /misc/*.jpeg
Allow: /misc/*.png
Allow: /modules/*.css$
Allow: /modules/*.css?
Allow: /modules/*.js$
Allow: /modules/*.js?
Allow: /modules/*.gif
Allow: /modules/*.jpg
Allow: /modules/*.jpeg
Allow: /modules/*.png
Allow: /profiles/*.css$
Allow: /profiles/*.css?
Allow: /profiles/*.js$
Allow: /profiles/*.js?
Allow: /profiles/*.gif
Allow: /profiles/*.jpg
Allow: /profiles/*.jpeg
Allow: /profiles/*.png
Allow: /themes/*.css$
Allow: /themes/*.css?
Allow: /themes/*.js$
Allow: /themes/*.js?
Allow: /themes/*.gif
Allow: /themes/*.jpg
Allow: /themes/*.jpeg
Allow: /themes/*.png
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
Disallow: /experiments/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
Disallow: /?q=experiments/
```

Илл. 2.20. Сплошные запреты!

Просто ради галочки я набрал www.company.com/admin и тут же разинул рот от удивления: без какой бы то ни было проверки мне дали к ней доступ! В папке хранились приватные файлы гендиректора компании. Судя по всему, он использовал ее, чтобы расшаривать документы, которые могли понадобиться ему в командировках. Там хранились контракты, банковские данные, фотография его паспорта и множество других данных, которые не должны быть доступны никому.

Я нашел контракт, подписанный всего несколько дней назад. Купил доменное имя (оно на два символа отличалась от названия реальной компании, с которой был заключен договор) и создал почтовый ящик на имя человека, который его подписал. А затем послал на адрес гендиректора письмо с прикрепленным зараженным файлом. «Прошу прощения, что делаю это уже после подписания контракта, но возник вопрос по п. 14.1а. Взгляните, пожалуйста, еще раз. Буду ждать ответа!» — было написано в моем письме.

Буквально через 15 минут генеральный директор открыл письмо и приложенный к нему файл. Затем написал на фальшивый адрес, что контракт никак не открывается. Пентест[11], на который должна была уйти минимум неделя, успешно завершился буквально через три часа.

Я позвонил гендиректору, и содержание нашей беседы было примерно следующим:

Я: Здравствуйте, Пол. Это Крис из компании Social-Engineer. Я хотел бы обсудить с вами пентест…

ГЕНДИРЕКТОР: Ха! Уже сдаетесь? Я же говорил, наша компания — крепкий орешек!

Я: Не совсем так, Пол. Дело в том, что в данный момент в моем распоряжении есть ваши паспортные данные, дата рождения, номера кредитных карт, доступ к банкам и удаленный доступ с полномочиями сисадмина. Я хотел уточнить: этого достаточно или вы хотите, чтобы я поработал еще неделю?

ГЕНДИРЕКТОР: Да ладно, я вам не верю! Вы ведь всего пару часов назад приступили! Скажите, какой идиот купился и дал вам удаленный доступ? Мне нужно сказать ему пару ласковых.

Я: Знаете, Пол… (Я запнулся, не зная, уместное ли сейчас время для шуток, а одна, весьма удачная, уже вертелась у меня в голове.) Я бы обошелся с ним помягче, он вообще-то хороший парень.

ГЕНДИРЕКТОР: Мда? И кто же это?

Я: Пол, это вы.

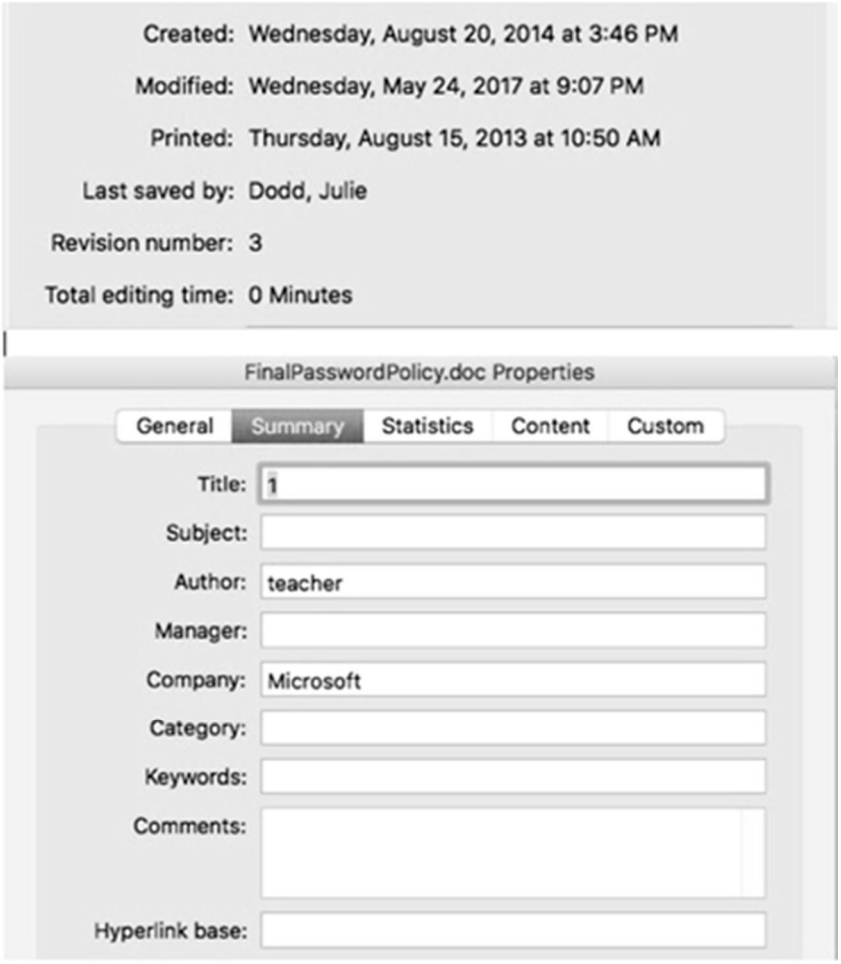
Тут я подробно пересказал ему свои действия, и он быстро все понял. Так что этот пентест был во многом обязан успехом файлу robots.txt и неправильно размещенной папке.

Все дело в метаданных, детка

Оксфордский словарь гласит, что приставка «мета» позволяет описывать «отсылку к себе или к общепринятым нормам типа “самореферентность”». То есть метаданные — это в буквальном смысле данные о данных. Отдает фильмом «Начало», вам не кажется?

Сейчас объясняю попроще. Метаданными называют информацию об объектах поиска. И в этих данных часто прячутся очень интересные факты, зачастую попадающие туда ненамеренно.

Представьте, что я провожу безобидный поиск в Google: ищу файлы с расширением .doc, в которых содержится информация о паролях. И вот я натыкаюсь на маленький документик с названием Final Password Policy («Политика в отношении паролей, финальная версия»). Что скажут мне метаданные? Давайте посмотрим на илл. 2.21.



Илл. 2.21. «Что у нас тут с метаданными??!»
(Обратили внимание, что я здесь сделал?)

Метаданные позволяют узнать время и место создания файла, имя последнего человека, который его сохранял, имя и должность его создателя, сколько раз его редактировали и др. Возможно, вы сейчас думаете: «Ну и что?»

Подобные документы способны предоставить социальному инженеру огромный объем информации. Только представьте, как в руки ему попадает документ о новой кадровой политике! Метаданные показали бы, когда этот документ в последний раз изменяли (в данном случае — месяц назад), кто его написал и когда его опубликовали. И конечно же, само содержание кадровой политики было бы внутри документа. Как думаете, открыл бы кто-нибудь файл, приложенный к фишинговому e-mail, отправленному от лица автора этого документа с пометкой о внесении изменений?

Посмотрите на илл. 2.22.

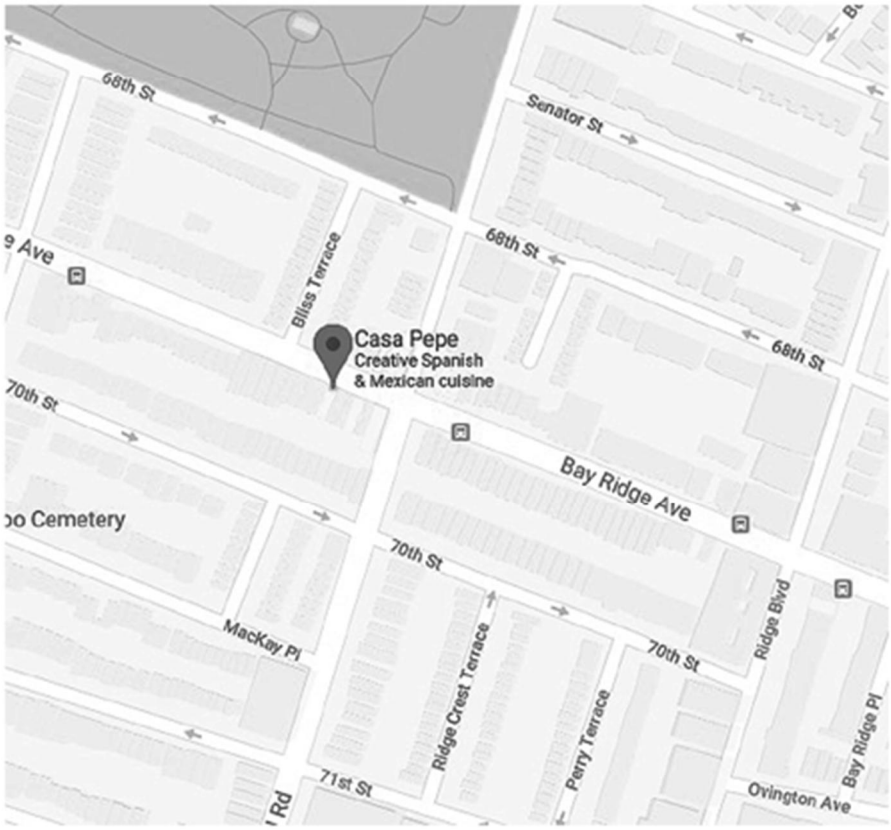
Сначала вы наверняка подумали: «Хм, мы что, будем тут устраивать фишинг по поводу купона на острый соус?». Нет. Обратите внимание на метаданные, изображенные на скриншоте 2.23.

Илл. 2.22. «Нет, серьезно, What's-a meta you»

Натыкаясь в интернете на безобидное на первый взгляд фото, не забывайте о метаданных — они сообщат, на какую камеру, когда и во сколько был сделан снимок, и даже выдадут GPS-координаты места, где этот снимок был сделан. Введите координаты в Google-карты и… см. илл. 2.24.

На карте мы видим парковку у ресторана Pepe's, в котором, кстати говоря, активно используют изображенный на фотографии соус.

Илл. 2.23. А вот и ответ



Илл. 2.24. Здесь довольно вкусно, если хотите знать мое мнение

Получается, кто-то сделал фотографию на смартфон. На смартфоне не был отключен GPS, а приложению камеры не запретили прикреплять метаданные к файлу с фотографией. И когда этот человек загрузил фото

в социальную сеть, эта информация оказалась доступна всем желающим.

Понимаете, к чему я клоню? А теперь представьте, что это информация не о вашем приятеле, который сходил в ресторан, а о:

- генеральном директоре крупной коммунальной компании, через которого планируют провести атаку национального масштаба;
- секретарше миллиардера, владеющей информацией о банковских счетах начальника и полномочиями по передаче средств;
- вашей пятнадцатилетней дочери, которая решила выложить в Сеть свои эротические фотографии.

Ну как? Вне зависимости от того, какой сценарий вам не понравился больше, понятно, что эта информация быстро становится опасной, если попадает в открытый доступ.

Однажды меня с моей командой наняли для проведения сбора данных из открытых источников и реализации атаки на высокопоставленного сотрудника организации, связанной с обороной. Перед нами не стояла задача его подставить, но необходимо было проверить, легко ли он решится на действия, совершать которые не следует. Чтобы в дальнейшем возможно было провести просветительскую работу, мы должны были записывать любые звонки сотрудника и регистрировать ссылки, по которым он перешел.

Нам не пришлось особенно стараться, чтобы найти его страницы в социальных сетях. Его Twitter оказался настоящей золотой жилой: он не просто активно там писал, но и использовал для этого свой новенький iPhone со включенным GPS. Почему это так важно? Благодаря геолокации постов сотрудника в Twitter мы составили график его передвижений в течение дня. Буквально за несколько часов мы узнали:

- где он любит пить кофе каждое утро;
- в какой спортзал ходит перед тем, как вернуться с работы домой;
- два его любимых ресторана;
- адрес его дома;
- как он ненавидит пробки.

Мы нашли еще много полезных данных в открытых источниках, однако именно эта информация определила вектор будущих атак. Во-первых, мы создали домен, который на одну букву отличался от адреса официальной страницы его спортклуба. Затем набросали электронное письмо, где сообщили, что в клубе якобы проводится обновление пользовательских аккаунтов, в ходе которого выяснилось: его кредитка не работает. Мы предложили ему «прямо сейчас войти в систему и самостоятельно обновить информацию о карте», подталкивая тем самым к быстрым действиям.

Конечно, мы знали, что по ссылке сотрудник увидит ошибку 404. Так что мы дождались, когда он перейдет по указанному адресу, и уже после этого позвонили. Диалог состоялся примерно такой:

СИ: Добрый день. Это мистер Смит?

Объект: Да, это я. А кто спрашивает?

СИ: Меня зовут Сара, я администратор спортклуба Cold's Gym. Сегодня мы отправили вам e-mail об обновлении системы, к которому прилагалась ссылка, к сожалению неработающая. И теперь мы обзваниваем клиентов, чтобы принести извинения за доставленные неудобства. Я могу сейчас выслать вам рабочую ссылку или же сразу обновить информацию по вашей карте. Как вам будет удобнее?

Объект: Все в порядке, Сара, сейчас скажу номер карты.

СИ: Спасибо, мистер Смит! И ждем вас сегодня на тренировку!

Эта атака сработала, потому что мы говорили о близких ему темах, и говорили убедительно. Просмотр открытых источников, один фишинговый e-mail — и мы заполучили клик по ссылке, номер кредитки и возможность простроить еще пять дополнительных векторов атаки.

Метаданные — мощный и очень полезный источник информации для социального инженера. Так что я настоятельно рекомендую анализировать их по каждому документу, который попадет вам в руки в процессе сбора данных из открытых источников.

Может показаться, что это слишком сложная задача, особенно если в вашем распоряжении окажется большой объем файлов. Лично я люблю использовать инструменты вроде FOCA (http://www.elevenpaths.com/labstools/foca/index.html) и Maltego (https://www.paterva.com/web7/), которые значительно облегчают задачу.

И несмотря на свое обещание не слишком углубляться в технологические дебри, я все же должен хотя бы коротко рассказать вам об этих полезных инструментах.

Орудия труда

Итак, в первой главе я сообщал, что не буду подробно описывать инструменты, потому что они слишком быстро обновляются и меняются.

Однако даже среди них есть образцы стабильности. Например, было бы нечестно не упомянуть четыре инструмента, которые я неизменно использовал в работе на протяжении последних пяти-десяти лет. И хотя эти инструменты существуют уже давно, их интерфейс и функционал постоянно меняются и модифицируются. Я мог бы разобрать их актуальную на сегодня функцию, но к моменту публикации книги эта информация наверняка устареет. Так что лучше просто укажу сайты этих замечательных продуктов, где вы сможете найти необходимые

руководства и узнать о самых горячих обновлениях. Обещаю провести для вас короткий, но необходимый для формирования полной картины экскурс.

SET

Помню, как однажды в разговоре со своим добрым другом Дэвидом Кеннеди я поделился мечтой: найти инструмент, который позволил бы мне в ходе подготовки фишинга автоматически создавать зараженные файлы, собирать личные данные или клонировать любую веб-страницу. Дэйв тогда ответил: «Думаю, я могу его создать».

С момента нашего разговора не прошло и 24 часов, а у Дэвида уже был готов прототип. И с тех пор Дэйв занимается SET (Social Engineers Toolkit, или «Набором инструментов для социального инженера») так, словно это дело всей его жизни. Он регулярно выпускает обновления (иногда кажется, что буквально каждый день). За последнее время в SET появились такие встроенные функции, что на их фоне оригинальная идея кажется просто ничтожной. Этот поразительный инструмент был скачан больше 2 млн раз.

Скачать SET, а также изучить прилагающуюся к нему инструкцию можно на сайте https://www.trustedsec.com/social-engineer-toolkit-set/.

IntelTechniques

Это скорее не отдельный инструмент, а целый ряд эффективнейших поисковых систем, которые объединил в одну программу мой друг Майкл Баззелл.

Майкл — признанный эксперт сразу в нескольких областях, но двумя из них он буквально живет и дышит. Первая — это поиск людей в интернете. А вторая — умение прятаться от тех, кто ищет тебя в интернете. Именно Майкл посоветовал мне открывать компании-однодневки в Мексике, если я вздумаю что-либо покупать через Amazon: чтобы невозможно было проследить мои передвижения через операции по кредиткам.

Майкл собрал удивительную коллекцию инструментов для поиска буквально везде: в социальных сетях, по номерам телефонов, IP-адресам и с помощью реверсивного поиска изображений. Взять все эти инструменты можно на сайте https://inteltechniques.com/menu.html, и я советую вам задержаться на нем подольше, чтобы подробно все изучить.

FOCA

FOCA — это аббревиатура от английского выражения Fingerprinting Organizations with Collected Archives (мощный инструмент для извлечения

и анализа метаданных; поиск цифровых отпечатков организаций через коллективные архивы). Этот инструмент, тут же притянувший к себе внимание всего интернета, представила на конференции DEF CON 18 небольшая группа хакеров из Бразилии еще в 2010 году.

В всем мире до сих пор не появилось достойных аналогов FOCA. За последние годы проект переживал взлеты и падения. В какой-то момент я даже перестал им пользоваться, потому что казалось, будто его прекратили обновлять, а связаться с создателями не представлялось возможным (создавался инструмент не на основе открытых источников).

Но потом проект перешел в руки ребят из компании Eleven Paths. Они обновили программу и презентовали ее на своем сайте https://www.elevenpaths.com/labstools/foca/index.html. К сожалению, программа разработана только для Windows. Но даже если вы используете другую операционную систему, имеет смысл настроить виртуальную машину.

FOCA обрабатывает файлы и извлекает из них полезные метаданные поразительно быстро. В общем, настоятельно советую ознакомиться.

Maltego: праматерь

Здесь я рискую произвести впечатление, будто создатели Maltego подкупили меня, ну да ладно. Дело в том, что я просто обожаю этот инструмент. Правда. То, что сделали его разработчики из Paterva, встретишь не часто: они выпустили небольшую бесплатную версию (тоже, кстати, шикарную), а коммерческую версию продолжают постоянно обновлять, так что проект не стоит на месте, он развивается и остается полезным.

Так что же такое Maltego? Это инструмент для хранения и визуальной систематизации данных из онлайн-источников. С помощью Maltego можно отслеживать, анализировать и выявлять связи между информацией, поступившей из разных публичных источников.

Maltego существенно облегчает мой труд, пользоваться этой программой легко и приятно. Кроме того, разработчики сняли отличные тренировочные видео и составили обучающие курсы. И вишенка на торте: Maltego подходит для любых операционных систем.

Вы можете сами познакомиться с этим инструментом и скачать его с сайта Paterva: https://www.paterva.com/web7/downloads.php#tab-2. Рекомендую начать с версии Maltego Classic.

Резюме

Нет сомнений в том, что знания — сила. И нет лучшего способа, чем сбор данных из открытых источников, чтобы сформировать эти знания об объекте воздействия. Если вы будете следовать описанным в этой главе

принципам, тренироваться и оттачивать перечисленные навыки, то научитесь находить в интернете даже мельчайшие крупицы важной информации.

Итак, представим, что вы собрали всю необходимую информацию из открытых источников, а затем аккуратнейшим образом ее систематизировали и задокументировали. Кажется, вы нашли все необходимое для определения вектора атаки. Пришло время перейти к подготовке легенды. Как анализировать собранные данные, чтобы найти в них главные индикаторы коммуникативного стиля объекта воздействия? Об этом поговорим в следующей главе.

3 Профайлинг через общение

(или как использовать слова собеседника против него же)

Чтобы эффективно общаться, мы должны понимать, что по-разному воспринимаем мир и руководствуемся этим восприятием в процессе общения с другими людьми.

Тони Роббинс

Во время работы над прошлым изданием этой книги я много времени посвятил обсуждению моделирования коммуникации с Крисом Никерсоном, владельцем компании Lares Consulting. Он в этом вопросе настоящий мастер и профи.

Крис помог мне погрузиться в тему и понять, как социальные инженеры воспринимают процесс коммуникации. Теперь я могу сказать, что моделирование коммуникации сводится к четырем основным аспектам:

- источнику;
- сообщению;
- каналу передачи;
- получателю.

Если хоть один из этих аспектов отсутствует, коммуникации нет. Основные модели коммуникации (например, модель Шеннона–Уивера или модель «ИСКП» Берло, где выделяются источник — сообщение — канал — приемник) отражают этот принцип.

За годы работы я понял: на практике не так уж важно, какую модель брать за основу. Знаю, знаю, сейчас кому-то из вас захочется бросить эту книгу в огонь. Но погодите, позвольте объясниться.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

В 1947 году Клод Шеннон и Уоррен Уивер разработали модель Шеннона–Уивера, которую теперь иногда называют «матерью всех моделей». Спустя почти 15 лет Дэвид Берло расширил их концепцию и создал модель «ИСКП». Позже Д.С. Барнлунд объединил и упростил эти инструменты, создав модель коммуникации, которая чаще всего

используется сегодня. Теория Барнлунда описана во втором издании книги «Теория коммуникации» (Communication Theory, Second Edition; Routledge, 2008) в четвертой главе под названием «Трансакционная модель коммуникации»).

Вот ссылка: https://www.taylorfrancis.com/books/e/9781351527538/chapters/10.4324%2F9781315080918-5]

Если вы примените описанные в этой книге принципы, связанные с понятиями раппорта, влияния на собеседника, профайлинга и т.п., и объект воздействия получит ваше сообщение — уловка сработает. Если вы будете использовать эти принципы во взаимодействии с человеком и при этом общаться с ним в соответствии с его коммуникативными предпочтениями — все пройдет ровно так, как вам хочется.

Понимаю, заявление смелое, и я не хочу, чтобы у вас сложилось впечатление, что этот процесс прост, как дважды два — четыре.

Часто дела обстоят намного сложнее, причем мы сами себе мешаем. Например, мне нравятся честность и прямота. Я не против, когда мне сообщают о моих ошибках и просчетах: это помогает мне стать лучше. Но и с другими людьми я обычно общаюсь таким же образом — из-за этого у меня возникают трудности с теми, кому такая прямота не по вкусу.

Не так-то просто менять коммуникативный профиль по щелчку пальцев (хотя кому-то это удается легко). Главная сложность возникает, когда мы начинаем чувствовать себя комфортно и расслабленно (потому что мозг выделяет те же химические вещества, выработку которых мы хотим стимулировать у объектов воздействия) и опрометчиво погружаемся в собственную «зону комфорта».

Приведу такой пример. Вспомните, как в юношестве (или в зрелости) вы пробовали что-то новое. Например, новую еду. Своих детей мы с женой с раннего детства просили не отказываться от новых блюд сразу и пробовать их, прежде чем принимать решение. Доедать было не обязательно, но мы объясняли: ты не сможешь понять, нравится тебе еда или нет, если даже не попробуешь ее.

Как-то раз мы всей семьей поехали в Гонконг. Когда пошли в ресторан, наша дочь обнаружила в меню блюдо под названием «Белый голубь». Она спросила, можно ли ей это попробовать. Сначала я хотел сказать: «Ты уверена? Голуби — это же такие грязные птицы!» Но тут же вспомнил, что мы с женой договорились поощрять любознательность детей.

Дочь заказала-таки голубя, а потом посмотрела на меня и сказала: «Пап, а ты возьмешь что-нибудь необычное?» Что же, меня всегда интересовали морские огурцы, хотя я не был уверен, что действительно хочу их пробовать. Но название у них вполне безобидное, верно?

На илл. 3.1 моя дочь жует своего голубя. К сожалению, фотографии моего лица в момент, когда я попробовал морской огурец, не сохранилось. Но вы легко можете его представить: оказалось, что морские огурцы — это огромные личинки, ползающие по дну.

К чему я рассказал историю о кулинарных похождениях нашей семьи в Гонконге? Какое отношение все это имеет к моделированию коммуникации? Понимаете ли, когда я попробовал морской огурец, мне стало ужасно неприятно (честно говоря, эти твари просто отвратительны), и я тут же захотел заказать какой-нибудь очень-очень американской еды. Почему? Она казалась мне знакомой и удобной.

Илл. 3.1. Да, голубь подается с головой

ЗАБАВНЫЙ ФАКТ

Морской огурец я пробовал четырежды. И каждый раз это блюдо оказывалось таким же отвратительным, как и впервые. Это никак не относится к моделированию коммуникации. Просто подумал, что вам будет интересно.

Во время общения происходит то же самое. Попробовав выйти из зоны комфорта и исследовать что-то новое, вы наверняка почувствуете дискомфорт и захотите вернуться обратно. Особенно если результат этого исследования окажется не особенно приятным. При этом важно не застревать и в зоне комфорта. Чем чаще вы пробуете новое, тем выше вероятность того, что арсенал ваших инструментов пополнится чем-то интересным.

Итак, чтобы вы составили представление о месте коммуникации в социальной инженерии, я затрону в этой главе следующие темы:

- Умение понимать, о чем думает человек, когда вы к нему только приближаетесь.
- Знакомство с моделью DISC (значение этой аббревиатуры вы узнаете совсем скоро).
- Определение собственного стиля по модели DISC.
- Использование DISC для достижения СИ-целей.

Умения, которые мы будем обсуждать в следующих главах, между собой никак не связаны. Однако все навыки, описанные в этой главе, взаимосвязаны, они дополняют друг друга. Давайте для начала разберемся, как понять, о чем думает человек, когда вы к нему только подходите.

На подходе

Когда я преподаю на своем пятидневном Продвинутом практическом курсе для социальных инженеров, у многих посетителей неизбежно возникают трудности на одном и том же этапе работы: они не понимают, как начинать общение с объектом воздействия.

Речь идет о тех самых первых решающих секундах, которые зададут тон всему, что случится после. Здесь я хотел бы рассказать вам одну особенно позорную историю из личной практики.

Однажды я вместе с моим другом Робином Дрейком общались после очередного занятия со слушателями курса — их было человек семь-восемь. И они попросили меня продемонстрировать: каково это — запросто завязать разговор с незнакомцем. Интерес студентов меня опьянил. Мозг плавился от дофаминового удара, который я, по-видимому, получил после целого дня преподавания, а уровень адреналина в крови подскочил от ожидания предстоящего успеха. Я уже предвкушал, как круто проведу сейчас мастер-класс применения навыков социальной инженерии.

Робин вызвался найти для меня подходящий объект — и выбрал невысокого мужчину: он сидел на стуле в полуметре от меня и читал, видимо кого-то поджидая. А у меня, надо сказать, рост под два метра.

Просто представьте себе эту картину и подумайте, как мне лучше было к нему подойти. Сзади? Конечно нет: это бы его только напугало. Спереди? Тоже нет — ему пришлось бы смотреть на меня снизу вверх, вытягивая шею, и это неудобное положение вряд ли способствовало бы установлению контакта. Так что же делать? Вот как бы вы поступили на моем месте?

Ну а я, после того как Робин указал мне на мужчину, без задней мысли, громко и со своим фирменным нью-йоркским акцентом произнес: «Добрый день! Можно задать вам вопрос?»

От неожиданности мужчина так сильно отпрянул, что потерял равновесие и упал назад вместе со стулом. Я бросился к нему, заливаясь краской стыда и переживая, что он ушибся: «Позвольте вам помочь». Я резко дернул стул вверх, но мужчина оказался намного легче, чем я думал, так что бедняга слетел на пол.

Он яростно зыркнул на меня и закричал: «Да оставьте же меня в покое! Вы чего?!» (правда, выражения он использовал далеко не такие литературные).

Бормоча извинения и понурив голову, я вернулся к студентам, которые к тому моменту готовы были уже лопнуть от хохота. А Робин от смеха даже прослезился.

За годы своей работы в подобные истории я попадал не раз. В результате они помогли мне сформулировать мысль, которая в корне изменила мое восприятие общения. Как, по-вашему, вы должны вести себя с собеседником, чтобы тому было комфортно и безопасно? Подумайте.

Представьте, что идете по улице и вдруг замечаете незнакомца: он направляется в вашу сторону и явно хочет что-то вам сказать. Что вы подумаете в такой ситуации? Мой опыт показывает, что обычно возникают четыре вопроса:

- Кто это?
- Чего он хочет?
- Он опасен?
- Сколько времени это займет?

Если в первые пять–десять секунд взаимодействия с человеком вам удастся ответить на них, это кардинальным образом повлияет на ваше дальнейшее общение. Такая идея прослеживается во многих разделах моей книги, так что оставьте на этой странице закладку, потому что вам придется периодически сюда возвращаться. Четыре вопроса напрямую связаны с темами, которые будут подниматься в книге дальше:

- ваша легенда (четвертая глава);
- первые слова, которые вы скажете (пятая глава);
- язык тела и мимика (восьмая глава).

Я даже изобразил эти вопросы на илл. 3.2, чтобы вам проще было их запомнить.

Конечно, я не утверждаю, что у всех в голове при встрече с незнакомцами возникают именно такие формулировки, однако смысл их будет примерно одинаковым. Если вы, как источник коммуникации, сумеете ответить на все четыре вопроса уже в первом своем сообщении, то его получатель почувствует себя спокойнее и расслабится.

Мошенники всех времен и народов знали это и разными способами добивались того, чтобы усыпить бдительность объекта их обмана, и только после этого приступали к своему нечестному делу (цели взаимодействия). Понимание этого механизма позволит вам не только развиваться как социальному инженеру, но и защищаться в ситуациях, когда эти техники будут применяться по отношению к вам.

Илл. 3.2. Четыре наиболее важных аспекта коммуникации

И первый шаг на этом пути — вычислить, какой стиль коммуникации свойственен конкретно вам. Внимание: мы подходим к одному мощному и в то же время очень простому инструменту для профайлинга в ходе коммуникации.

Вставьте DISC

В 1893 году родился Уильям Моултон Марстон. В возрасте 22 лет он получил степень бакалавра гуманитарных наук в Гарварде, через три года стал бакалавром права в Гарвардской юридической школе, а еще через три защитил там диссертацию по психологии. Затем Марстон устроился преподавать в Американский университет в Вашингтоне.

Во время учебы в Гарварде он, помимо прочего, занимался мониторингом кровяного давления у людей, которые врут. В 1915 году Марстон разработал аппарат для измерения давления в ходе интервью.

В 1917 году Уильям Марстон опубликовал результаты своих исследований — они были сенсационными. Как вы, наверное, уже догадались, именно так началась история использования «детектора лжи». В 1920–1930-е годы Марстон много преподавал и работал консультантом госслужб. Для своего времени это был уникальный человек, ведь психопатология его мало интересовала, а вот поведением большинства «нормальных» людей он был по-настоящему увлечен.

В 1928 году Марстон опубликовал книгу «Эмоции обычных людей» (Emotions of Normal People), а в 1931 году увидела свет его вторая работа — «Интегральная психология: Исследование ответа единицы» (Integrative Psychology: A Study of Unit Response). В этих публикациях и

была сформулирована модель DISC. Ученый искал способы, которые позволили бы измерить энергию поведения и сознания. И хотя тест, который я приведу ниже, не является его разработкой, именно Марстон стал специалистом, который впервые применил ее на практике в 1930-х годах. Случай был интересным: киностудия Universal Studios переходила тогда от немого кино к звуковому, и в первое время ученый помогал актерам находить более реалистичные жесты и мимику.

ЗАБАВНЫЙ ФАКТ

Марстон был известным сторонником феминистского движения. В молодости он изучал греческую и римскую классику, и его привлекла идея использовать античные сюжеты для иллюстрации идей на тему прав женщин. Так в 1941 году появилась знаменитая героиня комиксов Чудо-женщина. В 2006 году она украсила собой Зал славы комиксов.

Работы Уильяма Моултона Марстона перевернули мое восприятие социальной инженерии. Многие специалисты до и после него пытались понять, каким образом можно быстро создать психологический профиль собеседника, однако простое решение Уильяма Марстона пришлось мне особенно по душе. Я не психолог, и психологический профиль человека сам по себе мне мало что дает. Но я социальный инженер, и, поняв, как собеседник общается, я могу подобрать к нему волшебный ключик.

Что такое DISC?

Аббревиатуру DISC расшифровывают по-разному, но мне больше всего нравится такой вариант:

D : Доминирование/господство (Direct/Dominant)

I : Влияние/побуждение (Influencing)

S : Постоянство/устойчивость (Supporter/Steady)

C : Следование/уступчивость (Conscientious/Compliant)

Каждая из этих характеристик иллюстрирует определенный стиль коммуникации. DISC также часто визуализируют как геометрическую форму (например, см. илл. 3.3).

Илл. 3.3. DISC — наглядно

Знания об особенностях этих стилей коммуникации можно использовать для предсказания поведения собеседника. Попробуйте применить DISC — и вы обнаружите, что все люди предсказуемо разные.

Скажем, вам попался представитель D-типа, доминантный собеседник, который любит выражаться прямо. Такие люди говорят громко и оживленно, либо тихо и жестко, или же используют некий средний вариант. Но в любом случае в процессе общения они будут прямолинейны. И чем быстрее вы сможете определить коммуникативный профиль человека, тем эффективнее на него повлияете.

Когда я обучаю этим навыкам на своих курсах и слушатели задают мне вопросы, среди них есть два постоянных. Вот они:

Вопрос: Как определить свой стиль?

Ответ: Отличный вопрос, но ответить на него непросто. Подробно мы разберем эту тему в следующем разделе.

Вопрос: Может ли человек использовать сразу несколько стилей или их сочетание?

Ответ: Да. У многих из нас есть предрасположенность к разным стилям, и овладеть можно сразу несколькими. Некоторым людям комфортнее всего где-то на их пересечении. Кроме того, «любимые» стили могут со временем меняться.

И даже несмотря на то, что предлагаемый метод оценки можно считать довольно точным, не забывайте, что тестов со 100%-ной эффективностью не существует (по крайней мере, я таких не встречал). Их точность варьируется в зависимости от ответов человека и рассматриваемого сценария взаимодействия.

Этот метод — неотъемлемая часть моего социально-инженерного арсенала. Он действительно помогает приблизиться к использованию навыков, которыми владеют профи.

Но, прежде чем я перейду к теме использования модели DISC в СИ, мы должны обсудить с вами один вопрос, возможно самый важный. Поговорим о том, как определить ваш собственный стиль коммуникации.

Понимание себя — первый шаг к мудрости

Этот подзаголовок не просто красивая фраза, а основа истинного понимания процесса профайлинга[12] в коммуникации. Прежде чем стать мастером общения с другими, важно сначала понять себя. Сейчас я объясню эту мысль подробнее.

Для работы на кухне у шеф-повара должно быть много ножей. Скажем, у меня есть ножи с лезвием длиной 10, 20 и 25 см. Кроме того, у каждого лезвия своя форма и служат они для разных целей (см. илл. 3.4). Как думаете, какой нож лучше выбрать для шинковки капусты?

Илл. 3.4. Выбирайте с умом

Я бы выбрал четвертый нож справа: он весит достаточно, чтобы разрезать толстый кочан, и он достаточно длинный. При работе с таким ножом будет снижена нагрузка на руки и запястья. Я знаю: некоторые люди режут капусту простыми ножами (например, такими, как пятый и шестой справа). Но несколько минут шинковки — и у них начинают болеть запястья. Кроме того, риск пораниться этими ножами гораздо больше, чем моим. Когда мы понимаем, какие инструменты лучше подходят для выполнения той или иной задачи, когда знаем, как их правильно использовать и каковы их сильные и слабые стороны, у нас появляется возможность найти идеальное средство для достижения цели.

К модели DISC эта аналогия имеет прямое отношение. Под разные задачи подходят разные коммуникативные профили. Определите свой — и сможете понять собственные сильные и слабые стороны, научиться яснее доносить до других свои мысли и намерения. Ваши шансы на то, что вы не оттолкнете собеседника, увеличатся — а это крайне важное умение для профессиональных социальных инженеров.

Я рекомендую своим ученикам разные средства оценки доминирующего стиля коммуникации, однако чаще всего типирования по модели DISC

оказывается достаточно. Но, прежде чем вы побежите вводить поисковый запрос «типирование DISC», позвольте рассказать, почему этого делать не стоит.

Я изучил многие средства для онлайн-оценки и сделал вывод, что лежащий в их основе метод кажется мне несовершенным. Тестируемому предлагают прочесть предложение, а затем ответить на несколько вопросов. Например:

Представьте, что вы — начальник Криса, а он только что нарушил субординацию. Что вам следует делать в такой ситуации?

А. Тут же его уволить.

Б. Пошутить и забыть.

В. Подробно обсудить, почему он сделал то, что сделал.

Г. Постараться донести до него, почему его позиция вредна для общего дела.

Подобные вопросы плохи тем, что для ответа на них у вас может просто не оказаться знаний и опыта. Что, если вы никогда не занимали руководящих должностей или если вам не приходилось сталкиваться с нарушениями субординации? Одним словом, переменных слишком много. А вопрос сформулирован таким образом, что результаты могут оказаться нерепрезентативными.

Поэтому, если вы хотите узнать свой тип по этой модели, советую выбирать тесты, в которых приведены не сценарии, а отдельные слова. Выбирать предлагается те из них, которые больше или меньше подходят вам.

Например, из приведенного ниже списка выберите слова, которые, на ваш взгляд, лучше всего и хуже всего вас описывают. Даже если они не подходят вам идеально, выберите из предложенных вариантов те, которые характеризуют вас лучше и хуже всего.

ЛУЧШЕ ВСЕГО	ХУЖЕ ВСЕГО
Логичный	Логичный
Серьезный	Серьезный
Покорный	Покорный
Своевольный	Своевольный

Когда вам предлагается этот выбор, то приходится воображать ситуации, в которых вы на самом деле раньше не оказывались. Для многих это сложно. Поэтому я и рекомендую выбирать из пар слов: это позволяет ставить более точные оценки.

Я часто советую своим ученикам отвечать на вопросы, ориентируясь на то, как они ведут себя на работе. Ведь обычно в профессиональной и личной жизни мы ведем себя по-разному. Такой подход позволяет

составить полноценное и честное представление о коммуникативном профиле человека.

К сожалению, я так и не придумал, как организовать типирование по модели DISC для каждого читателя этой книги. Поэтому, чтобы продемонстрировать вам возможности этого инструмента, мне пришлось проявить креативность.

Взгляните на илл. 3.5.

Илл. 3.5. Понимание модели DISC

Внимательно прочитайте слова, размещенные за пределами круга, и ответьте на следующие вопросы:

1. Какой стиль общения вам больше по душе, прямой или непрямой? Стоп! Прежде чем отвечать, запомните: меня не интересует, что о вас думают другие, — я прошу вас честно оценить самих себя. Быстро ли вы переходите к делу или не торопитесь? Возникают ли у вас сложности, связанные с прямотой в общении, или она доставляет вам удовольствие? На основании своих ответов определите стиль вашего общения как «прямой» или «непрямой».
2. Вы больше ориентированы на решение задач или на взаимодействие с людьми? Когда вам на работе нужно выполнить задание, чему вы уделяете больше внимания: достижению поставленной цели или людям, которые могут вам в этом помочь? Ответив на эти вопросы, выберите соответствующую характеристику своего стиля: ориентацию на «задачи» или на «людей».

Я по результатам выполнения этого задания записал бы «прямой» и «задачи». На илл. 3.5 линии, связанные с этими характеристиками,

отсекают сферу «D — Доминирование». Видите, как быстро получаются результаты!

А теперь оцените себя. К какому блоку вы себя отнесете? На илл. 3.6 представлены более подробные описания.

Илл. 3.6. Модель DISC — подробности

Опять же, если говорить про меня, то, согласно описанию D-типа, меня можно назвать прямым, ориентированным на результат, твердым, волевым и напористым человеком. На самом деле так оно и есть: даже страшно от того, насколько точным получилось описание. Но что это дает мне с практической точки зрения?

Очень просто. Результат говорит о том, что я предпочитаю прямой коммуникативный стиль. Ведь как вы помните, мы говорим не о психологическом, а о коммуникативном профиле. А значит, он поможет разобраться с тем, как поменять предпочитаемые методы общения, чтобы усилить воздействие на конкретные объекты.

Итак, если вы ответили на вопросы моего теста, у вас должно было сложиться довольно точное представление о своих особенностях. Но что делать, когда речь заходит о профайлинге других людей? И как использовать эту информацию?

Использование модели DISC в своих целях

Типирование по модели DISC пугающе эффективно: члены моей команды применяли его для работы в соцсетях, при телефонном общении и даже по фото.

Робин Дрейке однажды поделился со мной историей о том, как составил коммуникативный профиль человека всего по одному его фотоснимку. А на фото было изображено вот что…

Представьте: перед вами фотография людной улицы в центре города, на которой случилось ДТП. Никто серьезно не пострадал, просто легкое столкновение. Прохожие бегут к машинам удостовериться, что с участниками аварии все в порядке. Объект стоит позади, не смотрит на происходящее, его плечи опущены, руки в карманах. Вот и все.

Если основываться на изложенной информации, то к какому типу по диаграмме DISC вы бы отнесли этого человека?

Вспомните, о чем я спрашивал вас выше. Ориентирован ли этот человек на людей или на задачи? Согласитесь, первый вариант не подходит. Значит, на задачи.

Прямое общение он предпочитает или непрямое? Окружающие сосредоточены на произошедшем, а он явно не обращает на него внимания, поэтому Робин предположил, что он сторонник непрямого общения.

Таким образом, объект можно отнести к нижнему левому сегменту (C) схемы, изображенной на илл. 3.6. Следовательно, он склонен к анализу, сдержан, точен, систематичен, придерживается своих границ. Он куда-то шел, и стоявшая перед ним задача была важнее происходившего вокруг. Язык его тела не свидетельствовал об общительности или напористости, так что его, без сомнений, можно отнести к типу C.

Такой профайлинг сослужил Робину добрую службу. Если вы прочитаете его книгу «Дело не во “мне”: 10 лучших техник быстрого установления раппорта с кем угодно» (It’s Not All About “Me”: The Top Ten Techniques for Building Quick Rapport with Anyone), вы узнаете, чем кончилось дело (спойлер: конечно же успехом).

На своих занятиях я обучаю людей проводить такую оценку за считаные минуты: сосредотачиваться на четырех аспектах DISC и относить человека к соответствующему типу. Но что делать, если ответить на какой-то из вопросов не удается?

DISC на практике

Предположим, вы не в курсе, на что я больше ориентирован: на решение задач или взаимодействие с людьми. Зато знаете, прямое или непрямое общение я предпочитаю. Что ж, и в этом случае вы все равно могли бы эффективно выстроить взаимодействие со мной как с прямым человеком, даже если бы я мог относиться как к D-типу, так и к I-типу.

То же самое можно было бы сказать, знай вы, что я ориентирован на задачи, а не на людей. Вы можете общаться со мной как с представителем D- или C-типа, и это будет лучше, чем если бы вы

выстраивали взаимодействие со мной как с представителем S-типа. Понимаете, как это работает?

Предлагаю выполнить небольшое задание. Перейдите на страницу моего друга Ника Ферно https://twitter.com/nickfx?lang=en (на английском).

ОБРАТИТЕ ВНИМАНИЕ Ник в Twitter пишет мало, так что вам, выполняя это упражнение, придется хорошенько подумать.

СОВЕТ ПРОФИ Выполняя подобный анализ профилей человека в соцсетях, важно помнить, что перепост чужих тестов ничего не говорит о коммуникативном стиле владельца аккаунта. Поэтому я рассматриваю только личные публикации пользователя.

Итак, как вы думаете, Ник ориентирован на задачи или на людей? Прочитайте его твиты и определите наиболее подходящую для него категорию. Я читал их и однозначно выбираю ориентацию на задачу. А вот как насчет прямоты? Хм… вопрос посложнее.

Давайте разберем содержание его твитов. Я вижу довольно прямые сообщения о вещах, а не о людях. Это подтверждает мое предположение о том, что Ник скорее относится к D-типу.

Но даже в отсутствие 100%-ной уверенности вы все равно подберетесь ближе к истине. Так, в случае с Ником вы можете спокойно заключить, что он больше ориентирован на задачи, чем на людей. И вполне достаточно будет сделать вывод о том, что он является представителем либо D-, либо C-типа.

Еще один профессиональный секрет: обращайте внимание на описания, которые человек употребляет в речи. Например, сопоставьте используемые в постах Ника слова, с характеристиками типов D и C. Какие из них лучше всего описали бы его твиты? Можно ли сказать, что они прямые, напористые, ориентированные на результат? Или скорее точные, систематические?

Читая его посты, я вижу скорее D, чем C. Значит ли это, что Ник в общении на 100% является представителем D-типа? Не совсем. Иногда люди меняют предпочитаемый стиль в зависимости от того, где, как и с кем общаются. Например, когда я выступаю в роли тренера, то предпочитаю общаться как I или D. Это удобнее для меня, для студентов — в общем, для всех участников процесса. Но если бы вы хотели как-то на меня повлиять, вам нужно было бы сначала понять, как я общаюсь в сфере, в которой будете пытаться оказать на меня влияние.

Запутались? Старайтесь не слишком много об этом думать. Ведь это лишь одна стрела в вашем колчане — средство, которое поможет подобраться ближе к объекту уже в первые минуты общения.

Возвращаясь к нашему примеру: предположим, по итогам анализа вы отнесли Ника к D-типу. Как использовать эту информацию в своих интересах? Чтобы ответить на этот вопрос, нужно разобраться, как стоит

общаться с представителем каждого типа — вне зависимости от того, занимаете вы по отношению к нему авторитетную позицию или нет.

Представитель D-типа в общении

Если вы собираетесь общаться с ним, используя «авторитетную» легенду:

- говорите прямо и открыто;
- устанавливайте четкие границы;
- будьте немногословны, придерживайтесь сути;
- отвечайте на вопрос «что».

Если ваша легенда предполагает скорее подчиненную позицию:

- делайте упор на «что», а не на «как»;
- предлагайте варианты, но акцентируйте внимание собеседника на результате;
- сосредоточьтесь на логике;
- соглашайтесь с фактами и мнениями, а не с человеком.

Представитель I-типа в общении

Если вы собираетесь общаться с ним, используя «доминирующую» легенду:

- будьте дружелюбны и расслабленны;
- пусть в основном говорит собеседник;
- помогите ему претворить идеи в действия;
- отвечайте на вопрос «кто».

Если ваша легенда предполагает скорее подчиненную позицию:

- делайте упор на новизну и уникальность;
- предлагайте компромиссы;
- не доминируйте;
- ссылайтесь на «экспертов» и свидетельства.

Представитель S-типа в общении

Если вы собираетесь общаться с ним, используя авторитетную легенду:

- старайтесь сохранять объективность, будьте систематичны;
- будьте расслабленны и дружелюбны;
- сохраняйте последовательность и отвечайте на вопрос «почему»;
- четко формулируйте, чего хотите.

Если ваша легенда предполагает скорее подчиненную позицию:

- будьте терпеливы;
- спрашивайте «как»;
- сосредоточьтесь на команде.

Представитель C-типа в общении

Если вы собираетесь общаться с ним, используя «авторитетную» легенду:

- рассказывайте подробно;
- произведите впечатление человека, на которого можно положиться;
- демонстрируйте уважение и признание;
- отвечайте на вопрос «как».

Если ваша легенда предполагает скорее подчиненную позицию:

- ссылайтесь на данные и статистику;
- будьте логичны, опирайтесь на факты;
- делайте упор на надежность.

А теперь давайте выполним небольшое упражнение, используя описания каждого из коммуникативных стилей. Предположим, что Мишель — представительница I-типа, а я — D. Что мне нужно изменить в своем подходе к общению, чтобы эффективнее на нее повлиять? (Можете видоизменить условия упражнения, поставив себя на мое место.)

Я обычно стараюсь опираться на факты, говорить кратко и по существу, но Мишель-то предпочитает дружелюбие и взаимные уступки при отсутствии явного доминирования. Видите, в чем заключалась бы сложность? Мне нужно создать легенду, которая одновременно удовлетворила бы Мишель и позволила мне оказать на нее влияние. Чтобы эффективно влиять на решения, которые принимают люди, нужно больше внимания уделять их желаниям, а не собственным предпочтениям в общении.

Разбираемся с ограничениями

Важным аспектом применения этой модели является среда, в которой происходит взаимодействие: общаетесь ли вы лично, по телефону, электронной почте или в социальных сетях. По сути, вам нужно определить коммуникативный стиль объекта воздействия, среду взаимодействия и цель общения, которую вы перед собой ставите. Дальше все, казалось бы, просто.

Пожалуйста, не воспринимайте эту модель как универсальную и единственно верную. Существует множество условий, от которых зависит успех или провал взаимодействия. Даже если вы правильно проведете профайлинг, верно оцените особенности объекта влияния и

сформулируете сообщение, которое тут же переместит его в зону коммуникативного комфорта — все это не гарантирует успеха. Болезнь, стресс, физическая усталость и многие другие факторы могут повлиять на способность человека к эффективной коммуникации. Не верите? Тогда вспомните своих детей (или детей ваших знакомых).

Дочка способна растопить мое сердце за секунду. Она обладает суперспособностью заставлять меня делать все что угодно. Но, когда я нахожусь в состоянии стресса или слишком измотан делами, я не так терпим и добр к ней, как обычно. В таких ситуациях я использую другой метод коммуникации — и точно так же под влиянием внешних обстоятельств меняется поведение любых других людей.

Тем не менее терпенье и труд, как известно, все перетрут. Поэтому, даже если у вас снова и снова не будет получаться подружиться с моделью DISC на практике, не прекращайте попыток. Когда у вас наконец все получится верно, вы убедитесь в том, что метод и правда действенный.

А вот вам еще одна история. После выхода первой книги меня пригласили на автограф-сессию. Я такого не ожидал и был очень удивлен, когда у моего стола собралась очередь читателей: они не просто заплатили за мою книгу, но и хотели узреть на ней мою подпись.

Я услышал от посетителей много добрых слов и в свой адрес, и по поводу книги. Один молодой человек целую минуту без остановки говорил, как книга изменила его жизнь: помогла ему в сложные времена и даже повлияла на выбор нового карьерного пути. Это так меня поразило, что я подумал: «Неужели это правда? Или это снова проделки Дэйва? С чего бы кому-то говорить так о моей книге?» Я слегка улыбнулся, поблагодарил парня и отдал ему подписанное издание. На его лице отразилось заметное разочарование. Но в очереди стояли другие посетители, так что я стал подписывать следующую книгу. Успели подойти еще четыре или пять человек, а юноша все стоял неподалеку, язык его тела явно говорил о том, что он раздосадован.

Наконец, еще один юноша протянул мне книгу на подпись со словами: «Хорошая работа, но я заметил у вас четыре серьезные ошибки, и еще столько же раз вы сослались на Wikipedia». Я улыбнулся ему и попросил посидеть рядом, пока все посетители не разойдутся — а там мы все обсудим.

Как только он сел за мой стол, первый парень бросился к нам. Теперь он был страшно разозлен и не стеснялся в выражениях. Он выпалил (используя ненормативную лексику, которую я тут цитировать не буду): «Я признался вам, что вы изменили мою жизни, что я ваш фанат — так вы меня просто отшили!!! А этот чувак говорит, что вы говно — и становится вашим лучшим другом???!?! Что за …?»

Я не нашелся, что ответить. Его злость меня ошарашила, хотя и была понятна. Я извинился и предложил ему тоже присесть и подождать,

чтобы пообщаться после мероприятия, но парень был слишком расстроен. Он развернулся и ушел.

И лишь позже, неоднократно проиграв эту сцену в голове, я понял, что в действительности произошло между нами. Молодой человек был ярким представителем I-типа и общался со мной соответственно: энергично, открыто, живо, дружелюбно и т.п. Его коммуникативный тип был так ярко выражен, что я — как истинный D — даже не понял, как реагировать: просто закрылся и двинулся дальше. А когда ко мне подошел второй читатель и сказал, что знает, как можно улучшить мою книгу, его коммуникативный стиль мне понравился и захотелось продолжить общение.

Как можно было решить проблему? Или даже: что нужно было сделать, чтобы она в принципе не возникла?

Общаться на уровне человека. Когда первый юноша подошел ко мне со своей хвалебной речью, мне нужно было:

- спросить, какой раздел книги ему помог;
- похвалить его (если бы я почувствовал, что могу сделать это честно и обоснованно);
- активно выслушать, а затем предложить ему подождать, потому что в очереди за ним стоят другие люди.

Такое поведение с моей стороны помогло бы ему почувствовать себя принятым и особенным, и он бы не решил, что я просто от него отвернулся. Итак, что я всем этим хочу сказать. Даже если вы совершите ошибку, прокрутите в голове произошедшее и постарайтесь сделать выводы на будущее. Учитесь на собственном опыте.

Резюме

Модель DISC — мощный инструмент, помогающий быстрее установить раппорт, сформировать между вами и объектом атмосферу доверия, заставить его захотеть вам помочь. Научитесь быстро «читать» людей, затем освойте навыки практического применения профайлинга, скорректируйте собственный стиль общения — и вам будет намного легче выстраивать коммуникацию с объектами воздействия.

Не стоит слишком усложнять этот процесс. Помните: даже если вы частично определите свойственный человеку коммуникативный стиль, это существенно повысит эффективность вашего взаимодействия с ним. В то же время DISC — это не волшебство. По щелчку пальцев гением моделирования коммуникации стать невозможно (да и, честно говоря, это в принципе далеко не всем дано).

Так что просто не ставьте перед собой такой цели. Достаточно стремиться смещать фокус беседы с себя на человека, стимулируя в его

голове нужные химические процессы (образование дофамина и окситоцина — веществ, которые я упоминал в первой главе). Так вы сможете установить доверие и раппорт, а это существенно облегчит ваш труд социального инженера.

Возможно, сейчас вы подумаете: «Да это же, по сути, рецепт превращения коммуникации в оружие».

И окажетесь не правы. На самом деле очень многие вещи, созданные в мирных целях, используются как оружие. И лучший тому пример — машины.

У меня есть любимая машина. Обожаю на ней ездить. Всегда хотел такую — и наконец стал ее счастливым обладателем. Но не думаю, что создателям этой модели Audi хотелось, чтобы их детищем управляли водители, скрывающиеся с места ДТП. Однако, согласно отчету Фонда безопасности дорожного движения Американской автомобильной ассоциации за 2016 год, в 11% случаев виновники стараются убежать от ответственности.

Машина — отличное средство передвижения, способное доставить вас из пункта А в пункт Б, и ее же можно превратить в смертельное оружие: все зависит от человека, который ее использует. С моделью DISC дела обстоят точно так же.

Когда я работаю в Social-Engineer, LLC и провожу свой пятидневный обучающий курс для социальных инженеров, то всегда руководствуюсь мантрой: «От встречи с вами собеседник должен почувствовать себя лучше».

Если помнить об этом, то знания, полученные благодаря этой книге, помогут вам не только защищаться от атак и находить мошенников, но и в принципе эффективнее решать встающие перед социальными инженерами задачи.

Определяя коммуникативный стиль человека, не ищите способов это знание эксплуатировать и манипулировать собеседником. Думайте о том, как изменить собственное поведение, как общаться с человеком на его уровне, чтобы взаимодействие с вами приносило ему удовольствие.

Попробуйте применить полученные из этой главы знания в общении с членами семьи и друзьями, прежде чем переходить непосредственно к социальной инженерии. И, когда вы убедитесь в том, что разобрались в теме моделирования коммуникации, пробуйте постепенно внедрять в общение запросы на действия, ожидаемые от собеседника. Одним словом, тренируйтесь.

А когда почувствуете, что у вас получается, — переходите к следующей теме, которая позволит вам подняться на кардинально новый уровень. Речь идет о легендировании.

4 Как стать кем угодно

Все, что вы можете вообразить, — реально.

Пабло Пикассо

Мне бы очень хотелось, чтобы, открывая эту страницу, читатели слышали саундтрек к фильму «Миссия невыполнима». К сожалению, такой технологии книгоиздатели еще не разработали. Поэтому я просто напоминаю вам о существовании мелодии, которая отлично подошла бы к этой главе.

Умение становиться кем угодно — или, выражаясь языком социальных инженеров, использование легендирования — это звучит соблазнительно и круто, даже сексуально. Давая определение легенде, некоторые люди не скупятся на негативно заряженные слова, такие как «ложь» и «обман». Однако я предпочитаю более нейтральную терминологию. На сайте своего проекта о социальной инженерии (https://www.social-engineer.org/framework/influencing-others/pretexting/) я предлагаю следующее определение:

Легендирование — это изображение себя в роли другого человека с целью получения приватной информации. Это непросто. Иногда удачная легенда требует разработки образа полноценной личности «с нуля» и его последующего воплощения для манипуляции объектом. С помощью этой техники социальные инженеры изображают людей, занимающих различные должности и принадлежащих ко всевозможным социальным уровням. Не всегда необходимо использовать легенду для решения возникающих перед социальным инженером задач. Однако за свою карьеру специалистам приходится создавать их неоднократно. В основе любой легенды лежит предварительное исследование.

Когда для выполнения задания мне нужно было проникнуть на семь принадлежавших заказчику складов, я решил изобразить инспектора пожарной безопасности. В другой раз, когда необходимо было пробраться в кабинет руководителя и в канцелярию компании, я выбрал легенду дезинфектора, специалиста по борьбе с тараканами. Чтобы проникнуть в здание третьей компании и получить доступ к центру мониторинга информационной безопасности и к центру управления корпоративной сетью, я притворился соискателем на вакантную должность, который пришел на собеседование. А уже в здании сменил эту роль на образ менеджера, приехавшего из другого штата. Кроме того, я успел побывать главой отдела управления персоналом, представителем телефонной компании — список можно продолжать еще очень и очень долго.

Не существует легенды, которая подошла бы для всех ситуаций: вот почему эта глава — одна из самых важных в моей книге. По большей части она посвящена обсуждению принципов легендирования и их практического применения в разных ситуациях: в телефонных

разговорах, переписке по электронной почте или в социальных сетях, при личном общении. А проиллюстрирую я все это подробным рассказом об одной, как мне кажется, весьма показательной операции.

В этой главе мы обсудим следующие правила легендирования:

- продумывать цели;
- отличать реальность от выдумки;
- знать, когда остановиться;
- по максимуму использовать краткосрочную память;
- находить подтверждения своей легенде;
- воплощать легенду.

Легендирование часто оказывается самым интересным этапом работы, но в то же время и самым опасным. Если вы не будете работать по вышеперечисленным правилам, последствия могут быть катастрофическими. Ниже я поделюсь с вами историями собственных успехов и провалов, связанных с легендированием.

Если хотите профессионально заниматься социальной инженерией, эти знания должны стать для вас ключевыми. Ведь именно они определяют разницу между достижением цели и поражением.

Принципы легендирования

Прежде чем перейти к подробному разбору каждого из принципов, хочу рассказать вам о технике, которая помогла не одному новичку в мире социальной инженерии: я имею в виду систему Станиславского, или актерскую импровизацию.

В разных городах проводятся найти курсы по такой импровизации, на которые могут записаться все желающие. Многие из приемов, которые дают на этих курсах, описаны и в этой книге. Однако у офлайн-курсов имеется неоспоримое преимущество по сравнению с книгой: на занятиях есть возможность получить опыт.

Там вы научитесь выходить из зоны комфорта, вживаться в роль — и на практике поймете, что требуется для успешного планирования и воплощения легенды. Я понимаю, что не каждый читатель этой книги сумеет найти подходящие курсы. Но и тем, кому это не удастся, не стоит расстраиваться: ведь можно купить DVD с курсом актерского мастерства от Уты Хаген (https://www.amazon.com/Uta-Hagens-Acting-Class-DVDs/dp/B0001Z3IHG) или же найти этот курс на YouTube. Это видео — отличный источник знаний, с помощью которого вы лучше разберетесь во всех шагах создания легенды и способах вжиться в роль.

И все же, даже если вы попадете на хороший мастер-класс по актерскому мастерству или посмотрите полезное видео, вам не обойтись

без изучения шести принципов освоения легенды. Давайте разберем их по порядку.

Первый принцип: продумывать цели

Инспектор по пожарной безопасности, дезинфектор, менеджер по управлению персоналом — я упомянул лишь несколько легенд из тех, что воплощал за свою профессиональную жизнь. Для начала расскажу, как я выбираю наиболее подходящую для конкретной локации или объекта воздействия роль.

Все начинается со сбора данных из открытых источников: я нахожу все доступные в открытых источниках факты о человеке или компании — их историю, новости, информацию о хобби, антипатиях, событиях и пр. (все это мы уже подробно разобрали во второй главе). Эти данные и помогают мне выбрать наиболее подходящую легенду. Однако есть еще один важный аспект, который играет решающую роль в этом выборе, — моя цель. Понимание, чего я собираюсь достичь в ходе операции, важнее даже обладания полной картиной специфики бизнеса, в который я буду внедряться. Позвольте проиллюстрировать эту мысль историей, которую я называю «Эскапада на 18-м этаже».

Меня наняли для проверки того, возможно ли человеку «с улицы» попасть в охраняемое здание, которым владела и управляла компания — производитель аудиоконтента. Но моим клиентом была не она, а фирма, арендовавшая 18-й этаж, — туда мне и нужно было попасть. Обычно посторонних людей в здание не пускали, лифты включались только по пропускам, а головной офис компании вообще находился в другом штате... Я принялся за дело.

На фазе сбора данных из открытых источников моей команде удалось собрать крайне мало фактов об именах и личностях сотрудников компании. Однако мы нашли имя регионального руководителя и некоторую информацию о его проектах. Кроме того, откопали документы на сервере, который компания явно не планировала делать публичным: инструкцию по технике безопасности, несколько внутренних писем, маркетинговые материалы по грядущим проектам и еще несколько случайных документов.

Какую легенду можно было бы выбрать, ориентируясь на эту информацию? Прежде чем читать дальше, попробуйте сами ответить на этот вопрос.

Может быть, вы выбрали роль мастера по ремонту лифтов? Это позволило бы попасть в здание, не вызывая подозрений у охраны. Или вы подумали о том, чтобы изобразить представителя головного офиса, без предупреждения приехавшего для проверки работы филиала? Или иной вариант?

Отлично. Теперь я сообщу некоторые подробности, которые помогут вам определиться с выбором. Кроме проникновения на 18-й этаж в мою задачу входила видео- и фотосъемка входов и выходов здания, любых незапароленных компьютеров, открытых документов и проектов, которые нельзя было бы найти в публичном доступе.

То есть мне нужна была легенда, позволявшая не только приближаться к компьютерам и столам, но и носить в руках камеру — или, по крайней мере, возможность куда-то установить скрытую камеру.

В этом контексте образ специалиста по ремонту лифтов оказался бы ужасным решением. Да, он позволил бы проникнуть в здание, но к цели я бы так и не приблизился.

Легенда представителя головного офиса, возможно, позволила подняться на этаж и даже пройти в кабинеты, но все равно предполагала бы определенные ограничения. Ведь чтобы такая операция прошла успешно, мне нужно было знать, кто работает в филиале.

Внимательно изучив инструкцию по технике безопасности, которую мы нашли в интернете, я узнал, что в компании предъявлялись строгие требования к дверям, ведущим на лестницу. Их категорически нельзя было держать открытыми. Более того, со стороны лестницы на них даже не устанавливали ручки.

Благодаря этой информации я выбрал легенду работника службы безопасности. Будто бы в другом отделении компании возникла проблема и меня направили в этот офис удостовериться, соблюдаются ли правила безопасности здесь. По моему сценарию, персонал отделения о визите проверяющего не предупреждали, чтобы никто не мог подготовиться и скрыть нарушения. А для отчета о проверке я якобы должен был снимать весь процесс на камеру.

Теперь вы понимаете, как четкое понимание целей помогает совершенствовать легенду? Именно благодаря ему я сформулировал легенду, которая помогла мне достичь СИ-целей, не вызывая ни у кого подозрений. Грамотно, правда?

Итак, пришло время перейти ко второму принципу. Дальнейшее развитие событий «Эскапады на 18-м этаже» поможет нам в нем разобраться.

Второй принцип: отличать реальность от выдумки

Этот принцип связан с особенностями памяти: намного проще запоминается легенда, основанная на реальности. Причем это касается и вас самих, и объекта воздействия. То есть необходимо использовать собственный опыт и знания, которые у вас уже есть или которые вы легко можете получить. Сегодня я часто говорю, что среди всех видов отношений сложнее всего имитировать отношения между отцом и дочерью. Однако сам я этого не понимал до тех пор, пока у меня не появилась дочка. Мне кажется, то, как я о ней рассказываю и что

ощущаю, когда нахожусь рядом, сымитировать невозможно. Не будь у меня дочери (а в мою задачу входило бы установление раппорта с отцом девочки), очень опасно выдумывать такую легенду. Но ведь можно с нежностью рассказать и о какой-нибудь любимой племяннице, верно?

Это я все к тому, что ваша легенда должна основываться на фактах, эмоциях и знаниях, которые у вас есть или которые вы способны без труда сымитировать. Поэтому с легендой, которую я рассматривал выше, я наверняка потерпел бы фиаско: ведь мои познания о работе лифтов, мягко говоря, ограниченны — как и возможности изобразить специалиста по их починке. Если бы у кого-то возникли ко мне вопросы, мой провал был бы гарантирован.

Кроме того, выбирая роль, я стараюсь использовать имя, на которое автоматически откликаюсь. Некоторые люди способны реагировать и на чужое имя, но большинству все же удобнее использовать свое или его вариацию.

И конечно же, в подавляющем большинстве случаев для работы «в поле» я выбираю мужские персонажи. Но в переписке, социальных сетях и даже по телефону мне приходилось бывать и женщиной.

ЗАБАВНЫЙ ФАКТ

Во многих американских компаниях действует правило, согласно которому сотрудники службы поддержки не должны задавать вопросов о том, какого пола звонящий. Так что если некая «Салли» звонит и говорит голосом Барри Уайта, что ж, значит, такая вот уникальная женщина эта Салли. А поставив под сомнение гендер звонящего, вы рискуете обидеть человека с необычным голосом. Зная это, я спокойно представлялся Кристиной и Лаурой, когда нужно было общаться с объектами по телефону.

Если же говорить о реалистичности с точки зрения объекта воздействия, то нужно выбирать легенду, которая позволит объекту оставаться в альфа-режиме (помните, мы обсуждали его в первой главе?).

Если объекту знакома тема (он понимает значение терминов, званий, контекста), вероятность того, что он не обратит внимания на потенциальную опасность, возрастает.

Так, в ходе «Эскапады» я использовал документ, который нашел в открытых источниках. Это позволило не демонстрировать какие-то неизвестные мне навыки, так что и «изнутри», и «снаружи» все ощущалось реалистично.

Впрочем, иногда, особенно при использовании реальных данных, бывает непонятно, когда же надо остановиться.

Третий принцип: знать, когда остановиться

Понимание того, когда пора остановиться (каких действий уже достаточно и еще не случился их перебор), действительно важная штука. На мой курс часто приходят люди, готовые ради убедительности легенды придумывать своему персонажу целую жизнь. Вплоть до таких подробностей, как праздничное меню на его 11-й день рождения.

Когда встанет вопрос, насколько подробной должна быть ваша легенда, помните вот что: людям будет интересно лишь то, какие действия им нужно предпринять для создания полноценного «социального контакта» в предложенных вами условиях.

Сейчас поясню. Как думаете, что было важно для объекта воздействия, с которым я общался в ходе «Эскапады» в роли инспектора по безопасности?

Ему было все равно, как зовут моих детей и собак, его не интересовало, что я ел на завтрак. Его беспокоили те четыре вопроса, которые я упоминал в посвященной профайлингу третьей главе:

- Кто это?
- Чего он хочет?
- Он опасен?
- Сколько времени это займет?

А теперь давайте подумаем, какие ответы на эти вопросы хочет получить объект воздействия, учитывая выбранную мной легенду:

В.: Кто это?

О.: Я — инспектор по безопасности. Руководство компании направило меня сюда для проверки соблюдения требований безопасности.

В.: Чего он хочет?

О.: Мне нужно 15 минут для проведения быстрой проверки.

В.: Он опасен?

О.: Быстро сделайте то, что я прошу, и мой визит никому не доставит проблем.

В.: Сколько времени это займет?

О.: Надеюсь, не больше 15 минут.

Все прочие подробности излишни, они вряд ли будут интересны объекту. Означает ли это, что не надо больше делать никаких заготовок? Вовсе нет. Вы все равно должны продумать основную информацию о своем персонаже на случай, если кто-то все же начнет расспрашивать у него подробности. Например, в моей итоговой легенде оказалась следующая информация.

Меня зовут Фил Уильямс. Я 40-летний инспектор по безопасности. Женат, есть ребенок. Домашних животных мы не держим, но собак и

кошек я люблю. Человек я довольно скучный: хожу на работу, а после иду домой. Я прожил столько-то лет в таком-то штате.

Легенда получился довольно скромной. Какую же информацию мне нужно было запомнить, чтобы не провалить задание?

- имя жены;
- имя ребенка;
- возраст ребенка;
- название штата;
- название города в этом штате;
- мою должность и какую именно работу я выполняю для компании.

На этом, в общем-то, и все. Пожалуй, можно было найти еще несколько подробностей, которые стоило бы обдумать. Но это — основные темы, которых я наверняка коснулся бы в ходе беседы с объектами воздействия.

Хочу привести пример ситуации, участник которой не смог проявить необходимое чувство меры. Однажды я обсуждал с учеником его невыполненное домашнее задание: ему никак не удавалось установить контакт с незнакомцами в общественных местах. Чтобы помочь студенту восстановить уверенность в себе после этой неудачи, я предложил вместе отправиться в холл ближайшей гостиницы: он будет общаться с незнакомцами, а я — наблюдать за его действиями, чтобы потом устроить «разбор полетов».

В холле мой студент подошел к женщине и мило заговорил с ней. На лице ученика сияла улыбка, да и вообще его поведение было весьма располагающим. Женщина откликнулась и пошла на контакт. Поначалу язык ее тела был таким же теплым и дружелюбным, как и его: бедра были повернуты к собеседнику (подробнее про язык тела мы поговорим в восьмой главе). Мой ученик спросил, откуда она, и женщина с воодушевлением ответила:

— Из Филадельфии.

Он изобразил удивление:

— Серьезно? Я тоже!

К сожалению, это было чистым враньем. Как только студент произнес эти слова, я почувствовал приближение катастрофы.

— Прекрасно! А где именно вы живете? — поинтересовалась женщина.

Тут мой ученик понял, что не просто напортачил, а провалил задание. Он смущенно пробормотал:

— Ну, знаете… Рядом с таким большим колоколом…

— С большим колоколом? Это вы про Колокол Свободы?

— Да-да, про него, — совсем смутившись пролепетал мой парень.

— Молодой человек, не знаю, что вы там задумали — но… во-первых, это ваше «рядом с большим колоколом». Серьезно?! Да в Фили нет ни одного человека, который бы не знал, как он называется! И, во-вторых, «рядом с большим колоколом» жилых домов вообще нет. На этом я хочу с вами попрощаться, — сказала женщина, развернулась и ушла.

А ученик подошел ко мне и сокрушенно сказал: «И так происходит каждый раз, когда я пытаюсь выполнить задание».

Я попросил его максимально подробно пересказать диалоги между ним и другими незнакомцами. И пока он говорил, я все яснее понимал, в чем его проблема: он сразу шел на поводу у собеседника, даже если не имел достаточных знаний для поддержания выбранного образа.

Информацию про свойственное людям племенное мышление (подробно мы рассмотрим его в пятой главе) он воспринял как прямое руководство к действию: если скажешь объекту воздействия, что принадлежишь к одному с ним «племени», значит, обязательно ему понравишься.

ПОЛЕЗНАЯ ИНФОРМАЦИЯ

А знаете, я не хочу заставлять вас ждать аж до пятой главы и прямо сейчас опишу в двух словах, что такое племенное мышление. Племенное мышление включается, когда мы пытаемся влиться в какую-то группу («племя») и используем для этого определенный стиль одежды и речи, придерживаемся особенных культурных традиций и т.д. Социальному инженеру лучше вливаться в «племя», а не заставлять людей подстраиваться под себя.

Отрицательным опытом моего ученика должен воспользоваться каждый из нас. Подробности легенды нужно всегда продумывать заранее. Например, чтобы стать «частью племени» женщины из Филадельфии, нужно было всего лишь сказать что-то вроде: «Фили? Ни разу там не был, но часто слышал, что туда стоит поехать. А вам что больше всего нравится в этом городе?». Это позволило бы продемонстрировать собеседнице заинтересованность и готовность слушать. И не пришлось бы изображать наличие в действительности отсутствовавших знаний.

Усвоив это правило, вы научитесь намного эффективнее использовать легенду в работе. А после успешного первого контакта люди обычно открываются и с радостью выдают много подробной информации — и о себе, и о нужном вам объекте. Запоминать все эти подробности бывает сложно, и об этой проблеме мы поговорим в следующем разделе.

Четвертый принцип: по максимуму использовать краткосрочную память

Такая ситуация наверняка случалась с каждым: вы познакомились с человеком, отлично поболтали, но к концу разговора совершенно забыли, как его зовут. Некоторым это серьезно мешает: ведь если

собеседник узнает об этом досадном обстоятельстве, то обидится и решит, что общение с ним на самом деле было вам не интересно.

Практика показывает, что большинству людей сложно удерживать в голове все детали беседы. Но с другой стороны, трудно произвести на собеседника положительное впечатление, в процессе разговора все время поглядывая в блокнот, чтобы ничего не забыть. Да и если собеседник заметит, что вы в этот блокнот что-то за ним записываете, у него как минимум возникнут нехорошие подозрения. Как выйти из такой ситуации, я расскажу в этом разделе моей книги — вот почему он так важен.

Все мы неоднократно встречали рекомендации типа: «В течение первых 20 секунд после знакомства постарайтесь как можно чаще повторять имя вашего визави — и оно запомнится». Это действительно работает — но только если исполнение совета органично вписывается в ситуацию. Однако представьте: минуту назад мы с вами познакомились, и тут вы начинаете безостановочно говорить: «Ох, Крис, Крис, Крис… М-да, Крис… Вас зовут Крис, понятно. Так, Крис, о чем мы говорили, м-м-м, Крис?»

Пожалуйста, не делайте так, если нам доведется встретиться.

И все же совет верный: проще запомнить имя человека, если повторять его — но только в осмысленном контексте. Когда в ходе операции «Эскапада» я вошел в здание и направился к лифту, меня остановила женщина-охранник: «Извините, куда вы идете?»

Я остановился и, зная, что эту беседу нужно будет внести в отчет, сказал:

— О, извините, мадам, — и, немного помедлив, продолжил: — Меня зовут Фил Уильямс, я из компании [название которой я разглашать не стану]. У нас здесь офис на 18-м этаже.

Она просмотрела список посетителей в своей папке и сказала:

— Извините, мистер Уильямс, но вашего имени нет в списке допущенных к посещению здания лиц.

— Конечно, так и должно быть. Ох, простите, что я не слишком вежлив, но как вас зовут? — я посмотрел на ее бейджик. — Клэр? Так вот, Клэр, приятно с вами познакомиться. — Потом я еще секунду помедлил и продолжил: — Знаете, Клэр, в одном из региональных офисов нашей компании произошел неприятный инцидент, связанный с нарушением установленных правил безопасности. И теперь меня направили с проверкой в остальные офисы, чтобы узнать истинное положение дел. Конечно, о моем визите никому не сообщали.

— Понимаю, — ответила Клэр.

— В отчете, который я должен буду представить, между прочим, есть раздел об обеспечении безопасности на входе в здание. Так что я с

радостью напишу, что вы идеально следовали протоколу. Имя ваше я запомнил, а как ваша фамилия?

Говоря это, я потянулся за блокнотом, чтобы записать туда ее имя. И она без задней мысли ответила:

— Фэрклей. Ф-Э-Р-К-Л-Е-Й.

— Просто замечательно, миссис Фэрклей. Очень рад, что проверка началась на такой позитивной ноте. Спасибо за то, что так ответственно подходите к выполнению своих обязанностей. Надеюсь, остальные сотрудники этого офиса так же эффективно следят за соблюдением требований безопасности.

А затем она сказала то, чего даже я не ожидал:

— Мистер Уильямс, а давайте я проведу вас на 18-й этаж по своему пропуску и вы проверите, оправдают ли сотрудники ваши надежды?

— Клэр! Я же могу так к вам обращаться?

Она кивнула, и я продолжил:

— Клэр, это было бы просто замечательно.

Она гордо прошлась со мной, своим новым другом, к лифту, открыла его своей карточкой и отправила меня на 18-й этаж.

— Большое спасибо. Скоро увидимся: я спущусь буквально через 15 минут.

Итак, на что нужно обратить внимание в этом примере?

- Я несколько раз упомянул имя женщины-охранника в самом начале общения.
- Я выбрал легенду, которая давала мне логичное основание все записывать.

И хотя эти техники действительно приносят чудесные результаты, не всегда получается применять их. Поэтому нужно держать в рукаве другие «тузы». Я, например, использую такие:

- Визитки. Обмен визитками с объектом воздействия — отличный способ сбора информации о нем. Но не стоит делать это сразу: обмениваться визитками лучше после установления раппорта или перед расставанием.
- Записывающие устройства. Иногда я веду видео- и аудиозапись процесса личного общения с объектами воздействия. И телефонные разговоры тоже записываю, чтобы не упускать деталей. Такие записи очень помогают в дальнейшем, особенно если компания-заказчик предварительно даст вам на это разрешение.

- Помощь партнера. Иногда бывает полезным взять с собой помощника: он будет держать в голове все подробности, пока я займусь решением других вопросов.

Эти приемы помогут восстановить все детали операции при подготовке отчета. Однако они не слишком полезны для запоминания информации, которая может пригодиться в процессе взаимодействия с объектом.

Поэтому вот вам несколько советов, которые помогут запоминать информацию по ходу дела:

- Тренируйте память. И делайте это как можно чаще. Старайтесь запоминать подробности всех ваших бесед (даже когда вам звонят и что-то предлагают продавцы или когда вы просто с кем-то болтаете) и мероприятий, в которых участвуете, пусть даже они никак не связаны с вашей работой: семейные праздники, вечеринки, встречи в офисе.

  Запоминайте цвет рубашки собеседника, какие он носит украшения, его полное имя и другие мелочи, на которые раньше просто не обратили бы внимания.

  Я сравниваю тренировку памяти с накачиванием мышцы: чем больше этим заниматься, тем сильнее она становится.

- Читайте. Я заметил: когда читаешь напечатанную на бумаге книгу, она запоминается лучше, чем та, что прочитана с экрана ридера. Конкретные книги для тренировки памяти я советовать не буду — читайте все, что вам по вкусу, просто не с экрана. Научных доказательств истинности своего наблюдения я привести, к сожалению, не могу. Но хочу сказать, что чем больше времени я посвящаю тренировке мозга, тем лучше он справляется с поставленными перед ним задачами. Кроме того, я периодически сажусь решать математические задачи — это тоже помогает развивать внимание к деталям и способности к их запоминанию.

У меня есть для вас еще один ценный совет. В свободную минуту не ленитесь кратко записать свои наблюдения в блокнот или на диктофон.

Когда Клэр посадила меня в лифт, я тут же достал из кармана свой смартфон и наговорил на диктофон все, что запомнил. Такие заметки помогают убить двух зайцев. Во-первых, они значительно упрощают процесс подготовки итоговых отчетов. Во-вторых, и это гораздо важнее, проговаривание информации помогает лучше запоминать ее.

Вот что я записал тогда в лифте:

Клэр Фэрклей, охранник. Рост около 160 см, блондинка, среднего телосложения. Носит белую рубашку и черные брюки. На груди слева у нее висит бейдж. На ее столе фото двух собак. Клэр использует

планшет. Установил с ней раппорт, похвалив исполнительность. Пропустила меня на 18-й этаж по своей HID-карте (висит на шнурке, прикрепленном к ремню справа). На лифте ввела код 4381.

Я только что записал все эти подробности по памяти, хотя события произошли больше двух лет назад. Думаю, теперь вы понимаете, почему я так уверенно рекомендую этот метод.

Следующий важный шаг на пути к созданию успешной легенды — поддержка.

Пятый принцип: находить подтверждения своей легенде

А теперь, пожалуйста, снова представьте себе во всех подробностях легенду, которую я привожу в пример на протяжении всей этой главы: роль инспектора по безопасности из крупной корпорации. Ответьте на вопросы:

- Во что он должен быть одет?
- Какие предметы должен носить с собой?
- Какими знаниями он должен в обязательном порядке обладать?

Эти вопросы и лежат в основе пятого принципа. Давайте ответим на каждый из них:

В.: Во что он должен быть одет?

О.: Практика показывает, что такие специалисты обычно носят штаны цвета хаки или простые джинсы. А также рубашки, застегнутые на все пуговицы, кроссовки или ботинки. А еще они всегда аккуратно пострижены.

В.: Какие инструменты должен носить с собой инспектор по безопасности?

О.: Насколько я знаю, такие люди носят с собой камеру, телефон, планшет, ручки и маркеры, бумагу для записей, инструкцию, а иногда и рулетку (но это зависит от конкретных задач).

В.: Какими особыми знаниями должен обладать такой человек?

О.: Чтобы ответить на этот вопрос, нужно сначала ответить на другие. Предполагается ли, что этот инспектор знает механизм работы огнетушителя? Должен ли он знать расположение пожарных выходов, сигнализаций и пр.? Или же он скорее просто может проверить их наличие в помещении? Что еще нужно знать о компании, в здание которой я пытаюсь пробраться? А что — о компании, сотрудника которой я изображаю?

Однажды нам с Мишель нужно было проникнуть в здание. Я вручил охраннику поддельную визитку, а тот вдруг спросил, где я живу. Как

выяснилось позже, это случилось потому, что название фирмы, указанной в визитке, охранник ни разу не встречал. Я такого вопроса не ожидал и потому указал на запад, сообщив:

— В том направлении.

— В промзоне? — удивился охранник. — А где же там жилые дома?

Я понял, что вот-вот попадусь, и попытался увильнуть от ответа:

— Нет, конечно, не в промзоне. Дальше, за ней.

— Извините, сэр, не хочу показаться грубияном, но на вашей визитке написано: «Семейное дело. Работаем уже 20 лет». И вы даже не можете сказать, где конкретно живете? — настаивал охранник, при этом очень уважительно ко мне обращаясь.

Недостаточно продуманная легенда определила мой провал: я не смог уверенно ответить на поставленный вопрос.

А ведь его можно было предугадать! Охранника, безусловно, стоит похвалить за внимательность. Я же на подобных глупостях больше не попадался. С тех пор, если на моей визитке был каким-то образом упомянут срок работы в компании, я всегда «готовил матчасть».

Однако чаще всего я упрощаю легенду: изображаю людей, которые только переехали или живут за городом. Это защищает меня от лишних вопросов местных жителей. В ходе «Эскапады» я убедился, что наличие планшета в руках позволяет не только выглядеть внушительно, но и записывать все, что посчитаю нужным. Ну а раз я выглядел убедительно, у Клэр не возникло сомнений в мотивах моих действий.

Вот так плавно мы и переходим к последнему принципу: воплощению. Если вы будете соблюдать все описанные выше правила, с ним, возможно, будет проще справиться.

Шестой принцип: воплощать легенду

Воплощение легенды не просто следование первым пяти принципам. Когда дело дойдет до реализации задуманного, могут возникнуть непредвиденные обстоятельства, нервное напряжение, да и предсказать поведение других участников процесса удается далеко не всегда. Случиться может все что угодно.

Я уже больше 10 лет работаю в социальной инженерии и до сих пор нервничаю перед началом каждой операции: не важно, предстоит ли мне войти в здание компании, поднять телефонную трубку и набрать номер или же просто нажать на кнопку, чтобы отправить электронное письмо. Не забыл ли я чего? А вдруг меня разоблачат? Вдруг я потерплю неудачу? Эти вопросы постоянно не дают мне покоя.

Вот что помогает воплощать легенду лично мне:

- практика;
- потянуться и подышать;
- общение;
- отказ от использования сценариев.

Важно помнить: даже если вы отлично подготовились, ваши планы могут нарушить непредвиденные обстоятельства, а они есть всегда. Это значит, что вам может попасться сверхнаблюдательный сотрудник, дотошный охранник или, вообще, закрытая на замок дверь. Иными словами, вы всегда должны быть готовы проявить гибкость.

Практика

Прежде чем пускать в дело фишинговый e-mail, я первым делом отправляю его самому себе и паре коллег, чтобы собрать обратную связь. Кроме того, прошу коллег перейти по ссылке или открыть приложенный документ, чтобы убедиться: все работает. Перед вишингом я обязательно проверяю, есть ли в моем распоряжении необходимые фоновые звуки, отображаются ли нужные данные на моем экране. Плюс к этому всегда совершаю тестовый телефонный звонок, чтобы убедиться: со спуфингом[13] все в порядке. Когда нужно отправить вирусное СМС-сообщение, я сначала посылаю его коллегам или самому себе, чтобы удостовериться: с форматированием все в порядке, ссылка рабочая. Если же мне нужно попасть в здание заказчика, стараюсь заранее довести до совершенства монолог, который планирую произносить перед охранниками и другими встреченными во время операции людьми. Также я наизусть запоминаю все детали еще до выезда на площадку. И конечно, проверяю «боеготовность» камер и другого оборудования, которое беру с собой.

Пол Келли, протеже доктора Экмана (о котором я уже писал во второй главе), однажды сказал: «Совершенная практика ведет к совершенству на практике». Тренируйтесь делать то, что вам нужно, чтобы добиться готовности на уровне мышечной памяти.

Именно практика зачастую определяет, что вас ждет: успех или неудача. Во время выполнения одного заказа я уже прибыл на место, достал оборудование из багажника и только тогда обнаружил, что в камере села батарейка. Я не проверил ее заранее. Пришлось использовать камеру в телефоне. Я очень переживал, сработает ли она, когда нужно, хватит ли заряда и не вызову ли я подозрений тем, что странно держу свой мобильный.

Потянуться и подышать

Кому-то это может показаться глупым, но во время задания я посвящаю несколько минут тому, чтобы потянуться и сделать несколько глубоких вдохов. Кроме того, в зависимости от степени внутреннего напряжения, я

могу на несколько минут даже принять властную позу, чтобы почувствовать себя увереннее в ходе атаки (в восьмой главе мы поговорим о таких позах подробнее).

Общение

Я всегда сообщаю необходимую информацию своим клиентам. Например, перед проведением фишинговой кампании обязательно предупреждаю контактное лицо о том, что атака состоится завтра. (Хотя, конечно, все зависит от условий заказа: в некоторых случаях я делаю это только постфактум.) То же самое касается и вишинга. Причем этот момент крайне важен в случае, если в ходе атаки я планирую имперсонацию. Я договариваюсь с контактным лицом о том, когда буду на месте, чтобы в случае, если что-то пойдет не так, можно было обратиться к нему.

Так, один раз меня поймали «с поличным». Хотя нет, не совсем так: сам клиент попросил меня сообщить охраннику, что я провел пентест — но уже после того, как я справился бы с задачей. Я несколько раз повторил, что считаю эту идею неудачной, но заказчик настоял на своем. В результате случилось вот что.

Я притворился специалистом по починке пресса для мусора и успешно проник на территорию компании, причем находился там столько, сколько мне требовалось, совершенно без сопровождения. На выходе я сказал охраннику:

— Сэр, прежде чем я уйду, мне нужно кое-что сообщить вам. Меня зовут Крис, а не Пол, как написано на бейдже. И я не тот, за кого себя выдавал. Я провожу так называемые пентесты: проверяю безопасность здания и эффективность систем защиты.

Лицо охранника покраснело от ярости, он потянулся к электрошокеру.

— Вы кто? Меня что, теперь уволят? — прошипел он.

Я попытался успокоить мужчину:

— Ну что вы, об увольнении речи не идет. Это всего лишь проверка, чтобы руководство компании могло разработать новые инструкции и усовершенствовать систему безопасности.

Но охранник не слушал меня, он вызвал по рации главу службы безопасности и нажал на кнопку, блокирующую двери, чтобы я никуда не убежал.

Когда пришел его начальник, охранник злобно начал описывать ситуацию, а когда я попытался вставить свои пять копеек, раздраженно закричал:

«С вами, Крис, Пол или как вас там, никто сейчас не разговаривает!»

Я ответил:

— Сейчас я покажу вам один документ, прочтите его, пожалуйста.

Я достал из кармана и отдал ему письмо, которое называю «спасающей от тюрьмы бумагой». В нем было подробно описано, кто я, что делаю и кто мне это разрешил. Кроме того, внизу значились номера телефонов людей, которые могли подтвердить мои слова.

Но, прочитав письмо, начальник охраны спросил:

— А как мне проверить, не подделка ли ваше письмо? А, Крис?

— Отличный вопрос. Вы можете позвонить по одному из указанных в нем номеров, — ответил я насколько мог убедительно.

— По этим номерам я звонить не буду. На том конце провода может оказаться ваш подельник, сидящий в фургоне неподалеку.

(«Черт, — подумал я. — А ведь он прав. Надо будет учесть это при подготовке к следующей операции. Спасибо, мистер начальник службы безопасности».)

— Я лучше позвоню человеку из руководства, которого знаю лично.

Он сделал это, и я услышал голос его знакомого в трубке: «Ничего я не знаю ни про какой пентест. Вызывай полицию!»

Меня отвели в служебный офис и заперли там в кладовом шкафу (серьезно!). К счастью, в спешке охранники забыли отобрать у меня телефон и отмычки. Так что через несколько минут я выбрался из шкафа, открыл дверь офиса, вышел в коридор и уже оттуда дозвонился своему контактному лицу, попросил его сейчас же разобраться с возникшей ситуацией. К счастью, днем ранее я предупредил его о планируемой атаке. Вскоре я уже уходил восвояси, причем обошлось даже без применения электрошокера.

Эта история показывает, почему так важно в нужное время сообщать нужным людям нужную информацию. Да, это звучит слишком обобщенно, ведь в нашей работе нет стандартных ситуаций: каждый клиент в каждой конкретной ситуации предъявляет нам свои требования и диктует особые правила. И одни клиенты гораздо больше нуждаются в обратной связи, чем другие. Так что просто помните: вы — профессиональный социальный инженер, и ваша задача заключается в том, чтобы клиент остался доволен.

Отказ от использования сценариев

Этот совет в первую очередь важен для представителей С-типа по модели DISC. Обычно они детально прописывают каждый шаг своих будущих действий (подробное описание коммуникативных профилей и модели DISC вы найдете, вернувшись к третьей главе). Когда вы используете сценарий в процессе вишинга или реализации легенды, то лишаете себя гибкости, динамичности. А я могу гарантировать только одно: ни одна атака не пройдет строго по плану. Так что умение

подстраиваться под обстоятельства существенно повысит процент успешных операций в вашем портфолио.

Резюме

Я рекомендую периодически повторять шесть правил легендирования и оттачивать навыки их применения. Помните: каждый последующий принцип основан на предыдущем. А вместе они помогут добиться большей эффективности в роли социального инженера.

Если вы научитесь правильно формулировать свои цели, то сможете создавать реалистичные легенды, поддерживающие объекты воздействия в бета-режиме (это я про исследования доктора Лангер, описанные в первой главе). Если вы будете использовать в легендах реальную, а не выдуманную информацию, вам будет проще добиться доверия. Затем решайте, насколько подробно стоит продумать роль для атаки — чтобы не переусердствовать и в то же время предусмотреть все необходимое. Чем проще легенда, тем лучше вы запомните не только факты о персонаже, которого играете, но и информацию, полученную в ходе операции. Правильное планирование облегчает выбор одежды, оборудования и техники, которую нужно использовать для придания легенде убедительности. Если все это вы сделаете как надо, воплотить задуманное будет несложно.

Пожалуйста, помните: продуманная легенда — залог успеха всей операции. Просто представьте, что было бы, появись я на объекте в деловом костюме, с портфелем и представившись мастером по ремонту пресса для мусора. Поверил бы мне кто-нибудь?

Да, я слегка перегибаю палку, но делаю это для наглядности. Если вы почувствуете, что вас могут раскрыть, вы начнете нервничать. Лишнее напряжение сделает вас менее находчивым и сообразительным, ухудшит память, а в нашей работе эти качества терять нельзя.

Правильно продуманная легенда поможет вашему объекту быстро ответить на четыре вопроса, о которых я говорил в третьей главе: кто вы, что вам нужно, несете ли вы угрозу и сколько времени займет взаимодействие с вами.

Впрочем, эти вопросы служат также и достижению другой цели — установлению раппорта. Этой теме будет посвящена следующая, пятая глава.

5 Я знаю, как тебе понравиться

Раппорт — это способность проникать в мир другого человека, формировать у него ощущение, будто вы его понимаете, будто между вами есть крепкая связь.

Тони Роббинс

Под ником OilHater[14] скрывался человек, до глубины души ненавидевший нефтегазовую индустрию. Образованный, умеющий грамотно и красиво излагать свои мысли, он «гастролировал» по соцсетям, рассказывая, как добыча нефти убивает экологию и губит Землю. Чем популярнее становились его посты и чем больше у него появлялось последователей, тем злее он писал.

ОБРАТИТЕ ВНИМАНИЕ В целях безопасности все имена в этой истории были изменены.

Несколько месяцев спустя, добившись устойчивой репутации, OilHater стал гораздо радикальнее. В своих постах он стал рассуждать о том, что остановить чудовищное разорение матери-природы можно, только уничтожая станции по проведению гидравлического разрыва пласта (ГРП): ведь этот метод добычи нефти считается самым варварским. Он даже упомянул несколько конкретных станций в Техасе, которые, на его взгляд, стоило стереть с лица Земли в первую очередь.

В то же время на те же форумы стал заходить Пол — отец двух маленьких детей, озабоченный опасностями, связанными с ГПР. В регионе, где жила семья Пола, начала разработки одна крупная нефтегазовая компания, и мужчина хотел узнать, как защитить своих детей от возможных негативных последствий.

Отзывчивые форумчане надавали Полу советов, как позаботиться о том, чтобы источники воды и почва в регионе не пострадали. По мере развития ситуации он продолжал общаться на форумах и задавать вопросы, обычные для новичка, не разбирающегося в теме.

Однажды на сообщение Пола развернуто ответил OilHater. В своем комментарии он даже подправил неточности, прозвучавшие в рекомендациях других форумчан. Пол поблагодарил OilHater’а за помощь, потому что уже порядком запутался в местами противоречивых советах от разных людей. Он также восхитился познаниями OilHater’а и поинтересовался, откуда у него столько информации: может, он сам работает в индустрии?

OilHater назвался простым неравнодушным гражданином, потратившим долгие часы на изучение деятельности нефтяных корпораций. Пол попросил разрешения задать OilHater’у пару вопросов в личном сообщении. В приватной переписке Пол рассказал OilHater’у, что живет в Техасе, очень интересуется вопросами нефтегазового производства и хотел бы знать, считает ли сам OilHater это дело настолько опасным, как описывали другие форумчане.

OilHater с удовольствием поддержал общение и принялся подробно описывать, насколько хорошо он разбирается в этих вопросах и как уверен в том, что технология ГРП действительно опасна. Пол взволнованно спрашивал, что же с этим безобразием делать. OilHater распалялся, Пол распалялся тоже. Он обращался к OilHater’у как к эксперту и буквально засыпал его вопросами.

Пола бесила мысль о том, что остановить ГРП-разработки никак нельзя, а значит, и спасти его детей от печальной участи — тоже. Как бы в шутку он написал OilHater'у:

— Складывается впечатление, что остается только стереть их с лица земли к чертовой матери. Как жаль, что это невозможно.

— А вот в этом я не уверен, — многозначительно ответил OilHater.

Пол поинтересовался, что OilHater хочет этим сказать, но тот надолго замолчал. Пол же продолжил писать на форумах, как его печалит и злит, что он и его живущая в Техасе семья попали в заложники нефтегазовой индустрии.

Примерно через неделю OilHater'а написал Полу в «личку», что нашел возможность защитить его семью от происходящего, что уже разработан план борьбы, но вот готов ли Пол участвовать в его воплощении?

— Это может быть опасно, — предупредил OilHater.

— Я готов пойти на риск ради спасения моих детей! Что именно ты задумал? — не смутился Пол.

— Чтобы разгрести беспорядок, иногда приходится испачкать руки, согласен?

— Безусловно. Но для меня главное, чтобы мои дети не заболели раком или чем-то похуже, пока эти мошенники загребают миллионы и плюют на простых людей!

— Помнишь, недавно ты написал, что единственный выход — стереть их с лица земли? Если это сделать, то на какое-то время работы по ГРП точно прекратятся.

— Я тебя внимательно слушаю. Никогда я раньше в подобное не ввязывался, но дети важнее страха. Как думаешь, что мы могли бы сделать?

— Знаешь кафе «У Пег» в центре?

— Конечно, постоянно там обедаю.

— Предлагаю обсудить это при личной встрече в четверг, в 19:30.

— С удовольствием. А как я тебя узнаю?

— Займи место в кабинке в заднем углу. Надень бейсболку. Я сам к тебе подойду.

Тут Пол засомневался:

— Извини, чувак, но это звучит как-то странно. Скажи хоть, как тебя зовут? Я — Пол Уилкокс, живу по адресу Главная улица, дом 123. Расскажи и ты о себе. Мне же нужно хотя бы знать, с кем я имею дело!

— Согласен. Извини за всю эту секретность. Просто я предпочитаю сохранять анонимность в Сети. Меня зовут Роберт Мур. Встретимся в «У Пег» в 19:30.

Но никакой Пол Уилкокс на встречу не явился. В 19:30 Роберт встретился с представителем правоохранительных органов, который позаботился о том, чтобы планы OilHater'а никогда не воплотились в жизнь.

Если вы еще не догадались, то Полом Уилкоксом был я. Тот проект, работа над которым заняла три с половиной недели, был основан на том, о чем пойдет речь в этой главе: как важно установить раппорт с объектами воздействия, заставить их себе доверять. Дальше, ссылаясь на эту историю, я буду называть ее «Операция "Нефть"».

В основу этой главы легли принципы, которые Робин Дрейке подробно описал в своей книге «Дело не во "мне": 10 лучших техник быстрого построения раппорта с кем угодно». Только Дрейке писал об использовании этих принципов в повседневном общении, а я продемонстрирую, как применять их в социальной инженерии.

Но, прежде чем мы перейдем к разбору этих принципов, хочу рассказать вам об одном аспекте «Операции "Нефть"», который и позволил мне установить раппорт с объектом. Этот аспект базовый, и, если вы в своей работе не учтете его, вас наверняка ждет провал.

Племенное мышление

Выполняя работу социального инженера, вам придется становиться частью «племени» объекта воздействия еще до того, как вы перейдете к установлению раппорта. Под племенем я подразумеваю социальную группу, которую можно идентифицировать по определенным признакам (например, одежде, общей цели, убеждениям или интересам). Общность членов группы и превращает ее в «племя». Следовательно, чтобы стать его частью, вы должны понять, что объединяет этих людей и как они распознают «своих» в разношерстой толпе.

Вспомните, например, старшеклассников: одежда подростка помогает понять, к какому «племени» он принадлежит.

В интернете можно найти видео под названием «Племенное мышление: ЭФФЕКТ ОЧЕВИДЦА (https://vimeo.com/265364702), которое наглядно демонстрирует, почему для каждого из нас важно в определенное время оказаться членом нужного племени. В сюжете снят эксперимент: одетый в повседневную одежду мужчина лежит на улице рядом с одной из самых загруженных станций метро в деловом квартале Лондона и зовет на помощь. Актер, изображавший мужчину, пролежал на земле больше 20 минут, прежде чем один из многочисленных прохожих решил ему помочь.

Но погодите, не осуждайте людей за их равнодушие, подумайте лучше о сюжете. Мужчина в джинсах, футболке и пальто лежит у выхода из метро, держится за живот и просит о помощи. Представьте себя на месте очевидцев, не знавших о том, что перед ними актер, и ответьте на четыре вопроса, которые мы разбирали в четвертой главе:

Кто это? Понятия не имею. Может, наркоман? Или мошенник? А вдруг ему и правда плохо? А я не заражусь чем-нибудь ужасным, если попытаюсь помочь ему?

Чего он хочет? Возможно, денег. А может, ему и правда нужна помощь — но я-то опаздываю на совещание. А вдруг он только и ждет, когда я замешкаюсь, чтобы вытащить у меня бумажник или вырезать почку?

Он опасен? Он ведь может оказаться вором или наркоманом. Я наклонюсь помочь, а он ударит меня ножом в живот. Или окажется, что он болен чем-то очень заразным.

Сколько времени это займет? Стаканчик для монет перед ним не стоит, так что можно влипнуть надолго. Вдруг придется везти его в больницу и потратить на это весь день?

У прохожих много вполне обоснованных сомнений. Они не находят четкого ответа на четыре вопроса и поэтому не спешат на помощь мужчине. А во второй части ролика показано, что происходит после того, как экспериментаторы меняют сценарий. Тот же самый актер так же лежит на земле — но теперь на нем деловой костюм. Как думаете, быстро ли ему оказали помощь? Где-то через шесть секунд. Когда людей, которые остановились, спросили, почему они это сделали, ответы были примерно следующие: «Ну, он был в костюме и я подумал, что ему и правда нужна помощь» и «Должно быть, ему действительно было плохо, раз он прямо в костюме упал на землю».

В ситуации изменилось только одно — одежда актера. Но эта деталь тут же определила ответы на четыре вопроса, которые задавали себе прохожие:

Кто это? Один из нас, и ему нужна помощь.

Чего он хочет? Помощь, и я готов оказать ее: ведь это такой же офисный работник, как и я.

Он опасен? Очевидно, нет — он слишком хорошо для этого одет.

Сколько времени это займет? Это не важно, потому что он «свой» и ему нужна помощь.

Учитывая место, в котором проходил эксперимент, костюм оказался тем самым аспектом, который позволил актеру продемонстрировать принадлежность к нужному «племени» и получить помощь. Да, племенное мышление — мощный фактор. Только подумайте: ведь существенных изменений, которые позволили бы с полной уверенностью ответить хотя бы на один из четырех вопросов, не произошло. Прохожие

не могли знать, кем на самом деле является лежащий незнакомец, сколько времени потребуется ему уделить и не окажется ли такое решение опасным. Они могли быть уверены лишь в одном: он просил о помощи.

По сценарию «Операции “Нефть”» я представлялся неравнодушным гражданином, которого бесила беззащитность перед нефтепромышленниками — а их, как мне было известно, объект воздействия ненавидел всеми фибрами души. Чем больше я «узнавал» о масштабах вреда, причиненного корпорациями, тем злее и беспомощнее мой персонаж себя чувствовал. И это сблизило нас с OilHater’ом.

И моя история, и эксперимент с мужчиной, лежащим на улице, прекрасно иллюстрируют возможности легендирования, которые мы обсуждали в четвертой главе. Правильно подобранная легенда помогает быстро решить задачу приобщения к нужному «племени». А после этого вы сможете применять 10 принципов установки раппорта, которые позволят достичь любой цели в процессе общения.

Раппорт в социальной инженерии

Что такое раппорт? Когда я задаю этот вопрос своим ученикам, они дают самые разные ответы. Многие говорят, что это «развитие отношений», «доверие» и «создание комфортной для собеседника атмосферы». Сам же я за годы работы скомбинировал из нескольких традиционных определений свое собственное:

Раппорт — это выстраивание моста для взаимодействия, основанного на доверии и общих интересах.

На мой взгляд, мост — отличная метафора. Все 10 описанных в этой главе принципов раппорта позволят вам как по мосту спокойно перейти в ряды «племени» объекта своего воздействия и доверительно с ним взаимодействовать. Но, прежде чем приступить к обсуждению этих принципов, нам с вами нужно разобраться, почему доверие играет такую важную роль в процессе общения.

Молекула морали

В 44-м эпизоде СИ-подкаста мне выпала честь пригласить в гости доктора Пола Зака. Как я уже говорил в первой главе, доктор Зак — автор книги «Молекула морали: Как работает доверие», в которой он описывает свои исследования окситоцина. Ученые долгие годы игнорировали этот гормон, но Пол Зак решил исследовать механизмы его выделения в кровь и последствия этого процесса.

В ходе исследований обнаружилось, что выброс окситоцина в кровь может быть обусловлен самыми разными причинами, но все они так или

иначе связаны с эмоциями, и в частности с ощущением доверия. В подкасте Зак поделился историей о том, как стал жертвой классической мошеннической схемы, для которой в английской языке есть даже специальное название — «pigeon drop», то есть «голубь обронил». Итак, в молодости Пол работал на автозаправочной станции. Однажды к нему подбежал взволнованный клиент и сообщил, что обнаружил в уборной шкатулку с драгоценностями. Как «добропорядочный гражданин» он якобы решил передать шкатулку Заку, чтобы тот сохранил ее и вернул хозяину — ведь тот обязательно объявится. И правда: вскоре на заправке зазвонил телефон: некий мужчина, явно пребывавший в отчаянии, говорил, что забыл в туалете шкатулку с фамильными драгоценностями. Радости его не было предела, когда Зак сообщил, что потеря буквально только что нашлась. В знак благодарности мужчина предложил выплатить $200 добропорядочному гражданину, который не стал забирать находку себе.

Когда Зак передал добрую весть посетителю, тот сказал, что дождаться приезда хозяина шкатулки не сможет, поскольку спешит на собеседование. Тогда человек на том конце провода предложил отличное решение: сейчас Зак даст благородному мужчине $100 из кассы — и тот поспешит на собеседование. Затем приедет хозяин украшений и отдаст обещанные $200. Половину из них Зак сможет взять себе, а еще $100 вернет в кассу. Конечно, никто с $200 на заправку не приехал, а драгоценности оказались фальшивыми. Почему же Зак поверил в этот обман?

Первый мошенник заставил Зака думать, что является членом его «племени», потому что доверился ему сразу в двух вопросах: он согласился отдать юноше половину вознаграждения за «драгоценности», а также «поделился» с ним ответственностью за найденную шкатулку.

Звонивший мошенник сделал так, чтобы Зак почувствовал свою принадлежность к особой группе доверенных людей. После этого мозг Зака выделил окситоцин и звонивший стал ассоциироваться у него с позитивными чувствами. Поэтому, когда он попросил выдать хорошему человеку $100 вознаграждения (из кассы), Зак с радостью согласился.

Много лет Зак не мог понять, как же повелся на эту уловку, до тех пор пока не начал изучать свойства окситоцина и писать свою книгу. Доверие заставляет нас совершать действия, которые, как мы прекрасно понимаем, на самом деле совершать не стоит.

Если вы будете применять описанные в этой главе принципы установления раппорта, то поможете мозгу — и объекта воздействия, и вашему собственному — выделить окситоцин. И объект почувствует к вам доверие. Но больше всего в результатах исследований доктора Зака меня удивило даже не это. А то, что эти ощущения могут вернуться к человеку, когда он будет вспоминать о действиях, ставших причиной выброса окситоцина. То есть в нашем случае он будет вспоминать о

взаимодействии с вами, если вы сумели эффективно установить с собеседником раппорт.

Еще одно важное химическое соединение, которое необходимо упомянуть в нашем обсуждении, — это гормон дофамин. Как Рене Ридль и Андрия Явор подчеркивали в своей статье под названием «Биология доверия: Интеграция данных из области генетики, эндокринологии и фМРТ» (Journal of Neuroscience, Psychology, & Economics, 2012, http://psycnet.apa.org/buy/2011-27428-001), дофамин является главным нейромедиатором системы поощрения. Кроме того, в этой статье отмечается, что комбинация дофамина и окситоцина играет особенно важную роль в социальных отношениях. По сути, дофамин и окситоцин являются важнейшей составляющей процесса доверия, а также позитивного подкрепления удачных социальных взаимодействий.

Теперь вы понимаете, почему так важно разобраться во всех этих дофаминово-окситоциновых процессах? Научившись устанавливать раппорт и вызывать у собеседника доверие, вы сможете выстроить мостик взаимосвязи между собой и объектом воздействия. По мере развития ваших отношений объект почувствует себя счастливее (чем до знакомства с вами), что, конечно, только укрепит вашу связь.

10 принципов установления раппорта

В 20-м эпизоде СИ-подкаста я отправился на тренировочное задание за город. Затем мы должны были встретиться с гостем подкаста в отеле и записать выпуск. Но в последнюю минуту гость отказался от участия. А я всегда гордился тем, что выпускал подкаст строго во второй понедельник каждого месяца, поэтому стал думать, кто из прежних гостей подкаста показал себя интересным собеседником. Кому я могу неожиданно позвонить и попросить срочно поучаствовать в этом выпуске?

И я быстренько настрочил e-mail своему товарищу Робину Дрейке: не выручит ли он меня? Робин тут же ответил: «Не вопрос! А что будем обсуждать?»

Даже толком не подумав, я ответил: «Лучшие техники быстрого установления раппорта с кем угодно».

Час спустя мы уже записывали подкаст, который не просто имел огромный успех, но и вдохновил Робина на написание его первой книги. На нашей встрече и позже, в книге, он осветил следующие 10 принципов:

- искусственные временные ограничения;
- невербалика;
- снижение темпа речи;
- сочувствие или помощь;
- усмирение эго;
- валидация[15];
- вопросы «как», «почему» и «когда»;

- взаимовыгодный обмен;
- равноценный альтруизм;
- управление ожиданиями.

В своей книге Робин подробнейшим образом разбирает каждый из них. Я же хочу осветить каждый принцип в контексте профессиональной деятельности социального инженера. И, где уместно, буду иллюстрировать их примерами из «Операции “Нефть”».

Искусственные временны́е ограничения

Создание временных ограничений предполагает, что вы каким-то образом ограничите общение с объектом по времени — тут все просто. Определение «искусственные» подразумевает, что этих ограничений на самом деле не существует и вообще-то вы могли бы взаимодействовать сколько вам заблагорассудится. Почему же этот принцип важен для социального инженера? Вспомните последний из четырех вопросов: «Сколько времени это займет?» Объект воздействия должен как можно быстрее получить ответ на него.

Искусственные временные ограничения помогают дать однозначный ответ. Поэтому, пусть даже полностью выдуманные, они должны казаться убедительными. Продумывая такие ограничения, нельзя забывать вот о чем:

- Если ваше ограничение окажется слишком жестким или необоснованным, оно вам не поможет. Например, вспомните известный вопрос: «Простите, можно вас на секундочку?». Понятное дело, за «секундочку» нельзя успеть ничего, так что подобные ограничения только обесценивают следующий за ними вопрос.
- Времени должно быть достаточно для реализации вашей легенды. Например, когда вы завязываете разговор с объектом в очереди в кассу в супермаркете, временное ограничение появляется автоматически: подойдет его или ваша очередь, и беседа завершится. Так что не нужно выдумывать ничего сверхъестественного — лучше работать в рамках временных ограничений, которые у вас и так есть.

В ходе «Операции “Нефть”» я использовал ограничения, связанные с обменом личными сообщениями в соцсетях. Если бы я слишком долго изливал свои «личные чувства», мне пришлось бы полагаться на то, что объект воздействия все это прочтет еще до установления между нами каких-либо отношений. Поэтому я писал кратко и по сути, но в то же время эмоционально. Тем самым я сформировал определенные временные границы для ответов OilHater’a: не заставлял собеседника напрягаться и спешить и в то же время показывал, что его ответы для меня важны и актуальны, и все это вместе способствовало

установлению между нами раппорта. Чем более личным и глубоким становилось наше общение, тем длиннее были сообщения.

Невербалика

Понять этот принцип в теории намного проще, чем применить его на практике. Для социального инженера эффективное использование невербалики подразумевает соответствие между языком тела и используемой легендой.

Предположим, вы пришли в любимый магазин вместе с ребенком. Рассматриваете вещи — и вдруг к вам обращается молодой человек, который явно куда-то спешит. Он говорит: «Извините. Я бегу на день рождения племянника и очень опаздываю. А подарок не купил! У него возраст примерно как у вашего сына. Можете сказать, сколько ему лет?».

Представили? А теперь ответьте, куда должен смотреть подошедший к вам человек? Пусть даже социальная инженерия тут пока ни при чем.

Должен ли он смотреть на вашего ребенка? Нет, это плохое решение. Когда незнакомцы рассматривают наших детей, у нас запускаются всевозможные «сигналы тревоги» и мы инстинктивно занимаем оборонительную позицию.

Тогда, может быть, он должен смотреть вам в глаза? Это, пожалуй, приемлемо, но не слишком соответствует запросу. А значит, может показаться опасным.

Логичнее всего молодому человеку в такой ситуации смотреть на товары или на дверь, потому что он ищет подарок и торопится. Теперь понимаете, что такое язык тела, подтверждающий слова?

Когда невербальные сигналы соответствуют сказанному, объект получает ответ на третий вопрос («Он опасен?»), а значит, раппорт устанавливается быстрее.

А вот еще одна причина, из-за которой этот принцип сложно применить. Я занимаюсь своим делом уже больше десяти лет — и все равно каждый раз страшно нервничаю перед взаимодействием с объектами — не важно, по телефону нам предстоит общаться или вживую. И если вы похожи на меня (а таких, как мы, кстати говоря, большинство), такое состояние наверняка отразится в напряжении вашего тела. Если же выбранная легенда никакого напряжения не предполагает, получится, что ваши невербальные сигналы ему противоречат (в восьмой главе мы обсудим тему невербальных сигналов подробнее).

Сложно бороться с собственными эмоциями, пытаясь сохранить реалистичность легенды (по крайней мере, если вы не социопат). Но социопаты не являются целевой аудиторией этой книги — она для будущих социальных инженеров. Так что велика вероятность того, что у читателей тоже возникнут трудности с невербаликой.

ЗАБАВНЫЙ ФАКТ

Майкл Томпкинс, кандидат педагогических наук и психолог Окружного центра лечения психиатрических заболеваний в Сакраменто, утверждает, что у социопатов есть совесть, однако она очень слабо развита. Так, социопаты могут без труда понять, какие их поступки не являются правильными, если им это на руку. Недостает им в первую очередь эмпатии — важнейшей составляющей человеческого общения.

Я не предлагаю вам заранее прописывать сценарии невербальных сигналов, которые вы будете подавать объектам воздействия в ходе операции. Однако советую продумать ту манеру своего поведения, которая покажется объекту логичной в рамках выбранной вами легенды. И очень важно не забывать об этом в процессе взаимодействия!

Касается это не только ситуаций непосредственного личного общения, но и вишинга. Если в ходе телефонного разговора вы примете неправильную позу, мышцы вашей гортани перенапрягутся, что повлияет на голос. Собеседник сочтет это напряжением, и установить с ним раппорт не удастся.

Но в ходе «Операции “Нефть”» переживать мне об этом по понятным причинам не пришлось.

Снижение темпа речи

Что происходит, когда человек пытается слишком быстро рассуждать на незнакомую или неудобную для него тему? Он запинается. Сами собой появляются слова-паразиты: «типа», «в общем», «как бы» и т.п. Слушая такую речь, невольно думаешь, что собеседнику недостает знаний или уверенности.

Такое же впечатление можно произвести, если говорить слишком медленно, есть даже риск показаться снисходительным. Одним словом, нужно найти оптимальную скорость речи.

Как это сделать? Вам помогут четыре критерия — Р.С.Г.В.:

Р.: ритм;

С.: скорость;

Г.: громкость;

В.: высота.

Внимательно прислушайтесь к собеседнику и оцените его речь по этим критериям. На получившиеся показатели и ориентируйтесь.

ПРЕДОСТЕРЕЖЕНИЕ Когда будете наблюдать за Р.С.Г.В. в чужой речи и пытаться соответствовать этим критериям, не пытайтесь имитировать акцент собеседника! Каким бы талантливым имитатором вы себя ни считали, делать этого не стоит (единственное исключение может быть в том случае, если вы денно и нощно трудились со специалистом над

отработкой всех возможных нюансов конкретного акцента). Плохая имитация акцента просто убивает раппорт, она может обидеть собеседника. Вместо акцента можно использовать типичные для конкретного региона слова и выражения. Например, американцы говорят не «метро», а «subway», а британцы — «tube». Большой сэндвич с мясом, сыром и помидорами я не задумываясь назвал бы «hoagie», а уроженец Бостона — «grinder». Используйте местный жаргон: так легче сойти за своего, а после можно будет применить и подстройку по Р.С.Г.В.

Социальному инженеру не стоит забывать об этом принципе, к тому же он логично сочетается с предыдущим. В идеале ваша речь должна соответствовать и критериям Р.С.Г.В. собеседника, и выбранной вами легенде. Если вы изображаете претендента на вакансию, который пришел в отдел по управлению персоналом, то ваше полное спокойствие и слишком уверенное поведение будут выглядеть скорее подозрительно: люди, которые приходят наниматься на работу, обычно волнуются.

Сочувствие или помощь

Исследователи Мартин Шульте-Рутер, Ганс Маркович, Гереон Финк и Матина Пифк опубликовали поразительное исследование под названием «Зеркальные нейроны и механизмы мышления, активизирующиеся при личном взаимодействии: Изучение эмпатии с помощью МРТ» (Mirror Neuron and Theory of Mind Mechanisms Involved in Face-to-Face Interactions: A Functional Magnetic Resonance Imaging Approach to Empathy) (https://www.ncbi.nlm.nih.gov/pubmed/17651008). В нем описывается эффект, который на человека производит запрос, вызывающий эмпатию. Согласно результатам исследования, достаточно посмотреть на нуждающегося человека, чтобы активизировались зоны мозга, связанные с эмоциональным переживанием боли.

Иными словами, если вы сумеете грамотно выстроить запрос на симпатию или помощь, у собеседника возникнет сильная эмоциональная связь с вами. Настолько сильная, что он вряд ли откажет вам в помощи.

Этот механизм отлично знаком маркетологам. Вот почему в тот момент, когда в рекламе звучит целевой запрос, они используют видеоряд и/или фоновую музыку, вызывающие определенные эмоции. Удивительно, но это работает не только при личном взаимодействии. Да, когда люди видят лицо просящего, эмоциональная связь оказывается сильнее, но обязательным условием это не является. Иногда одного только голоса или яркого описания бывает достаточно, чтобы объект воздействия представил себе определенный образ и ощутил эмпатию.

Социальные инженеры могут очень эффективно использовать этот принцип в работе. На протяжении всей человеческой истории преступники, мошенники и даже серийные убийцы использовали симпатию и призывы к помощи, чтобы заманить своих жертв в ловушку.

А сейчас я дам вам универсальный совет: уровень запрашиваемого у объекта содействия должен соответствовать уровню уже установленного между вами раппорта. Как думаете: если недавний знакомый и друг детства одновременно попросят вас помочь им с переездом в другую квартиру — чью просьбу вы удовлетворите? Скорее всего, в первую очередь вы поможете давнему другу: уровень раппорта между вами высок, вам не жалко потратить время и силы на такое дело. Если же малознакомый человек попросит о слишком крупной или слишком личной услуге, эффект будет прямо противоположным: раппорт ослабеет, могут даже возникнуть подозрения.

Проиллюстрировать это я хочу на примере «Операции “Нефть”». Первое время мои запросы на сочувствие и помощь выражались в том, что я просил людей объяснить мне технологию гидроразрыва пласта — ведь я якобы переживал за здоровье своих детей. Причем я не направлял свой запрос напрямую объекту воздействия, скорее это был призыв, адресованный всем, кто сам захочет откликнуться.

После того как OilHater показал себя «самым знающим» источником информации по интересующей меня теме, я стал формулировать прямые просьбы помочь мне. Чем дольше мы общались, чем сильнее становился раппорт, тем более подробные и личные вопросы я обращал к нему. В результате у меня появилась возможность использовать мощную модификацию принципа, которую называют «обратной социальной инженерией». Иными словами, мне не пришлось применять никаких классических трюков из мира СИ, чтобы сделать OilHater’а податливым — раппорт, который я так тщательно выстраивал, буквально заставил его мне доверять и делиться информацией.

Пол Зак говорит: окситоцин (та самая молекула доверия) активнее всего выделяется, когда объект чувствует, что может вам доверять. Именно на доверии выстраивается эта связь. Этот фактор оказывает мощное влияние на весь процесс общения, и его необходимо учитывать, когда вы что-то просите у объекта воздействия. Мне удалось применить этот принцип во время «Операции “Нефть”». Когда OilHater поверил мне настолько, чтобы раскрывать свои идеи, можно было сказать, что наши отношения стали крепкими как сталь. Я постоянно просил у OilHater’а о все большей помощи, а затем сам помог ему, когда потребовалось, — и в результате между нами установился очень сильный раппорт.

Усмирение эго

Этот принцип установления раппорта очень важен. Если вы его освоите, то вас уже будет не остановить. И все же этот принцип далеко не так прост, как кажется.

Чтобы было понятнее, в чем здесь заключаются основные сложности, хочу сначала прояснить, что я называю усмирением эго: это отказ от потребностей быть первым, правым, умным, отказ даже от своих

представлений о том, что такое хорошо и что такое плохо. Отрешаясь от эго, вы отбрасываете все эти мысли в сторону ради другого человека. А изобразить это ох как непросто.

Почему же этот принцип одновременно так важен и так сложен в применении? Многие чувствуют себя слабыми, когда признают, что чего-то не знают. А как обычно изображают слабых? В СМИ, в кино, вообще в искусстве смиренные и кроткие люди зачастую оказываются в роли жертв. Мне кажется, многим так сложно усмирять свое эго именно потому, что им не хочется показаться слабаками.

Приведу пример. Представьте, что стоите в очереди в супермаркете и краем уха слышите разговор за спиной. Кто-то говорит: «Из очень надежного источника слышал вот что: чтобы избавиться от всех аллергий, нужно три раза в день умываться молоком с медом и родниковой водой».

Многие понимают, что у этого утверждения нет научных обоснований. Что вы подумали, когда его прочитали? Если что-то вроде «Это пополнит список самых глупых советов, которые я когда-либо слышал» или «Этого человека нужно поправить», значит, до усмирения эго вам пока далеко. В противном случае вы бы реагировали примерно так: «Что же, вот такое у человека мнение. Да и пожалуйста! Попробую-ка понять, почему он считает именно так, а не иначе».

Усмирение эго — это восприятие мыслей, утверждений и мнений другого человека. Вы станете считать их подходящими вне зависимости от того, согласны с ними или нет.

В ходе «Операции “Нефть”» я смог применить этот принцип, когда изображал, будто ничего не знаю о методах работы нефтегазовой индустрии и ГРП (хотя, честно говоря, особо притворяться мне и не пришлось). Кроме того, я не ставил под вопрос мнение OilHater’а, какими бы ужасными, опасными и радикальными ни казались мне его высказывания. Я отодвигал свое эго в сторону и вел себя так, словно OilHater здесь главный и все решает. Когда социальному инженеру удается усмирить собственное эго и в то же время раздуть эго объекта воздействия, он создает идеальные условия для установления раппорта.

Есть еще одно условие успешного применения этого принципа — наличие определенных знаний по теме и умение задавать хорошие вопросы. Если социальный инженер показывает, что его знания ограниченны, но задает при этом интересные вопросы, он уступает объекту воздействия доминирующую позицию в общении. Я использовал эту технику в «Операции “Нефть”», когда продолжал снова и снова просить у OilHater’а дополнительные данные, которые помогли бы мне разобраться в тех крупицах информации, что у меня уже были. Его эго раздувалось, а мое — наоборот.

ПРИМЕР ПРЕЗИДЕНТСКОГО УРОВНЯ

Отличный пример применения этого принципа продемонстрировал один из бывших президентов США Рональд Рейган. Когда он баллотировался на второй срок, многие СМИ выражали сомнение в его способности справиться с президентскими обязанностями в силу возраста.

Рейган мог спорить и пытаться доказать неправоту своих критиков во время дебатов. Но он знал, что часто попытки оспорить мнение несогласных только подливают масла в огонь. Чем больше борешься — тем больше у них укрепляется уверенность в своей правоте. Так что Рейган выбрал другой подход: он сам постоянно затрагивал тему своего возраста, подшучивая над собой. Например, он мог сказать: «Я еще помню времена, когда репортеры, узнав про горячие новости, неслись в редакцию с криками: “Погодите, отложите штихели!”». Такой юмор Рейган использовал и в своих речах, и на пресс-конференциях.

Как бы журналистам ни хотелось выступить по поводу того, что Рейган слишком стар, чтобы снова становиться президентом, тот поднимал эту тему раньше и тем самым брал ситуацию под контроль. Если бы кто-то из журналистов решил пошутить над возрастом президента после того, как он сделал это сам, подобные нападки выглядели бы глупо. Иными словами, Рейган не расстраивался, а усмирял свое эго и обезоруживал противников юмором.

Валидация

Этот принцип тесно связан с предыдущим. Валидация предполагает, что вы соглашаетесь, хвалите или как-то иначе поощряете высказывания, решения и выбор другого человека. В ответ на это мозг собеседника выделяет дофамин и окситоцин, которые способствуют установлению между вами доверия и раппорта.

Помните, как я рассказывал о возможностях использования сочувствия и помощи? Правило, которое я тогда упоминал, действует и в контексте валидации: ее уровень должен соответствовать уровню раппорта.

И чтобы это доказать, приведу пример: расскажу о своем провале эпического масштаба. Давным-давно, когда профессиональная социальная инженерия еще была для меня в новинку, мне нужно было проникнуть в одно здание. Итак, я вошел через двери и оказался перед постом дежурного, это была женщина. На ее столе — штук десять фотографий в рамках, причем повернуты они были не к ней, а к посетителям. Снимки, сделанные явно во время каникул, запечатлели двух девочек со счастливыми лицами. Я сделал вывод, что женщина очень гордится своими детьми и хочет, чтобы их увидели все.

Я решил импровизировать в надежде быстро установить с ней раппорт и совершил грубейшую ошибку. Глядя на фотографии, я произнес: «Ммм, у вас такие красивые дочки…» И лишь через секунду сообразил, что девочкам на снимках лет 12–15, и моя фраза звучит весьма двусмысленно, с очень нехорошим подтекстом. Я растерялся из-за

случившейся неловкости, да и женщина тоже явно не оценила комплимент.

Она отодвинулась от стола, и удивление на ее лице сменилось сначала страхом, а потом злостью. Женщина поблагодарила меня, но скорее строго, чем вежливо, а потом спросила, кто я и чего хочу.

Я стоял перед ней и чувствовал, как на моем лице отражаются шок и смятение. Затем пробормотал: «Извините, я кое-что забыл в машине, сейчас вернусь» — и поскорее ушел. Конечно, возвращаться я не стал; пришлось выбрать другой день для проведения пентеста и отправлять на задание коллегу.

Помимо того, что я брякнул глупость, которая насторожила мою собеседницу, я предварительно не добился установления между нами раппорта, достаточного для того, чтобы озвучивать комплименты ее детям. А ведь с точки зрения валидации уместнее было бы сказать что-то вроде: «Судя по фото, вы отдыхали в каком-то райском местечке. А где это?» Или даже: «Какие красивые снимки! А наших детей попробуй сфотографируй!»

Вывод: при первом взаимодействии с объектом уровень раппорта будет близок к нулю. Поэтому валидация не должна быть слишком личной.

СОВЕТ ПРОФИ Убедитесь, что знаете о всевозможных культурных барьерах, когда речь заходит о подарках или комплиментах. Потому что нарушение культурных границ способно разрушить раппорт. В то же время их соблюдение помогает выбрать правильную форму валидации.

Помните, я здесь рассказывал, насколько мощным инструментом становится валидация, если использовать ее вместе с усмирением эго? Ведь в этом случае вы позволяете другому человеку проявить его эго. Ощущение валидации способствует установлению раппорта и выделению тех же химических веществ (дофамина и окситоцина). Таким образом, вы дарите собеседнику массу приятных ощущений.

В «Операции “Нефть”» я применял валидацию постоянно:

- усмирял собственное эго;
- валидировал действия и идеи объекта;
- восхищался эрудицией объекта;
- слушал его советы и, когда нужно, просил пояснить непонятное;
- принял его представления о том, как можно «решить» проблему.

Чем чаще этот процесс повторялся, тем сильнее укреплялся раппорт между нами.

Вопросы «Как?», «Почему?» и «Когда?»

Почему для установки раппорта особенно важно задавать именно такие вопросы? Потому что на них нельзя ответить коротким «да» или «нет».

Такие вопросы еще называют «открытыми» — ведь они служат для вовлечения человека в беседу.

А когда вы спрашиваете мнение человека и затем выслушиваете его ответ, это тоже воспринимается как валидация.

ПРЕДОСТЕРЕЖЕНИЕ Задав открытый вопрос, обязательно нужно внимательно выслушать ответ. Если человек начнет делиться своим мнением, а на вашем лице отразятся скука и нежелание слушать, это разрушит все шансы на валидацию. Так что когда собеседник что-то вам рассказывает, не стоит в это время проговаривать в уме собственные блистательные речи.

Открытые вопросы помогают поддерживать разговор. Зачастую небольшая пауза после заданного вопроса только подталкивает человека продолжать говорить — при условии что вы в это время проявляете явный интерес: то, что психологи называют «активным слушанием».

Впрочем, перебарщивать и спрашивать много раз подряд «почему» тоже не стоит — иначе вы рискуете стать похожим на трехлетку-почемучку. Они, конечно, милейшие создания, но для установления раппорта между взрослыми людьми это не лучший вариант.

В «Операции “Нефть”» я постоянно использовал вопросы «как», «почему» и «когда». Например: «Почему ГРП так вреден для окружающей среды?» и «Как же помешать им разрушить мою жизнь?».

Такие вопросы помогли OilHater’у раскрыться и поделиться со мной своими знаниями по теме. «Активное слушание» в режиме онлайн дается намного проще, чем в реальной жизни, потому что никто не мешает вам свериться со справочниками и разобраться в написанном, прежде чем отвечать собеседнику. Однако даже если вы планируете работать преимущественно онлайн, навыки активного слушания все же стоит отточить. Например, мой друг Джим Манли очень злится, когда отправляет мне письмо из восьми абзацев, в которых подробно описывает проблему, а я прочитываю первые предложения и тут же задаю по ним вопросы. Обычно он пишет мне что-нибудь в духе: «ХАДНАГИ, ПРОЧТИ ПИСЬМО ЦЕЛИКОМ!!!» (оригинальный текст пришлось подвергнуть цензуре). Если в этом вы похожи на меня, вам обязательно нужно отрабатывать навыки активного слушания, в том числе и в письменном общении.

В ходе «Операции “Нефть”» с помощью активного слушания и открытых вопросов мне удалось разговорить объект воздействия.

Взаимовыгодный обмен

Этот принцип можно еще назвать «дашь на дашь». Вот скажите, вам доводилось испытывать синдром раскаяния покупателя? Это когда вы на что-то потратились и в момент покупки были этому очень рады. Но когда

пришли домой и вскрыли упаковку, задумались: «А действительно ли покупка того стоила?»

Такое раскаяние возникает из-за ощущения, что товар не стоит потраченных на него денег. И одна из грубейших ошибок, которую может в своей работе допустить социальный инженер, — это оставить объект воздействия после общения именно с таким ощущением. Человек будет думать: «Да уж, отлично мы сегодня поговорили с… Стоп, а звали-то его как? И откуда он вообще? Так, то есть я ему представился, назвал дату рождения, показал фото детей и даже водительские права — а сам и имени его не узнал?!»

В результате таких размышлений у человека могут возникнуть страх и тревога, потому что ваш вклад в общение будет казаться ему неравноценным его вкладу. Причем, обратите внимание, именно казаться, а не быть. Согласитесь, это совершенно разные вещи.

По условиям одного моего задания мне нужно было подойти к объекту воздействия в магазине, где тот находился со своим сыном. Следуя правилу, которое мы обсуждали выше, я обратился к нему, посматривая на прилавки: «Извините… Я очень опаздываю на день рождения племянника. Жена меня просто убьет, если я не привезу подарок, а я про него совсем забыл. Племянник по возрасту как ваш сын. Не подскажете, во что дети в этом возрасте играют?»

В этом высказывании я заложил основу для взаимного обмена информацией, потому что сообщил ему, что:

- Я женат.
- У меня есть племянник, а значит, брат или сестра с детьми.
- Я опаздываю.
- Я еду на день рождения.
- Я ничего не понимаю в детях.

Пара коротких предложений — а объект обладал таким количеством информации обо мне, что по завершении общения вряд ли почувствовал бы «раскаяние покупателя», ведь он теперь «хорошо» меня знал.

СОВЕТ ПРОФИ Вам не обязательно сообщать реальную информацию о себе (имя, количество детей и т.п.). Но помните: чем больше выдуманных подробностей, тем больше вам придется запоминать. Поэтому социальному инженеру я всегда рекомендую соблюдать принцип «чем проще — тем лучше».

В «Операции “Нефть”» я несколько раз использовал принцип обмена информацией, однако особенно удачно это получилось, когда OilHater назначил встречу в кафе «У Пег». Я первым сообщил ему свое имя и домашний адрес, чтобы вызвать к себе доверие и пробудить в нем желание ответить взаимной честностью. Что он и сделал — а я в результате смог предотвратить преступление.

Равноценный альтруизм

Представьте себе салазковую пилу и механизм ее действия: лезвие движется вперед и назад, туда и обратно. По такому же принципу работает и раппорт. Отправить свой альтруизм «туда» можно через слова или действия, предполагающие, что вы даете объекту воздействия что-то важное. И затем он тоже отдаст что-то важное вам.

Например, если вы пропустите человека вперед и придержите ему дверь, за которой окажется еще одна дверь, как думаете, что сделает он? Конечно же, придержит дверь для вас. Это и есть равноценный альтруизм. Как применить его в социальной инженерии? Если вы дадите человеку что-то ценное, он или она окажутся в моральном долгу перед вами и постараются этот долг отдать. Но важно еще и вот что: кто определяет ценность того, что было дано?

Ответ однозначен: получатель, не вы. Определить, что конкретный человек посчитает ценным, можно с помощью открытых источников, наблюдения или обобщения. Но какой бы метод вы ни выбрали, не советую ориентироваться на собственные ценности. Если же вам удастся дать объекту воздействия нечто, на его взгляд, очень ценное, он будет чувствовать себя в таком долгу перед вами, что может даже проигнорировать протокол безопасности.

Однажды я пришел по очередному заданию в здание одной компании и, когда приблизился к посту охраны, заметил, что сидящая за столом женщина выглядит так, будто только что плакала. Я на секунду переключился с СИ-режима и спросил:

— С вами все в порядке?

Беспокойство мое было искренним, она это заметила, а потому честно ответила:

— Сегодня я пришла на работу в сережках, которые муж подарил мне на нашу десятую годовщину. Он много лет копил деньги, чтобы их купить. Они такие красивые, а я взяла и потеряла одну! — и женщина снова заплакала.

Я предположил, что сережка могла упасть на пол, и тут же наклонился, чтобы ее поискать. Женщина сделала то же самое, приговаривая:

— Я уже здесь все обыскала. Хотя хуже не станет, если проверю еще раз.

Тут в окно заглянуло солнце и я заметил, что за плечом у женщины что-то блеснуло.

— Вы, наверное, уже смотрели, но мне показалось, у вас на плече сзади что-то блестит. Позвольте, я проверю?

Она повернулась, и я снял с ее свитера зацепившуюся бриллиантовую сережку — действительно прекрасную. Женщина снова заплакала,

теперь уже от радости. Она обняла меня и поблагодарила так горячо, что мне даже стало неловко.

А потом сказала:

— Боже мой, я же отняла у вас кучу времени! Чем я могу вам помочь?

Тут я понял, что пора срочно переключиться обратно в СИ-режим — ведь что бы я у нее сейчас ни попросил, она наверняка исполнила бы это.

— Не стоит. Вы были так расстроены, что я с радостью помог вам. Но вообще-то я уже опаздываю на встречу в отделе кадров, так что, пожалуй, побегу.

Я взял свои сумки, папки и направился к закрытой двери. Причем шел я так уверенно, будто знал, что без проблем пройду. И — о чудо! — когда я подошел, послышалось механическое жужжание открывающегося замка.

Сам того не ожидая, я сделал женщине, которая отвечала за охрану, настолько ценный подарок (сережку, которой она очень дорожила), что ей было неловко после этого задерживать меня из-за каких-то глупых протоколов безопасности — ведь я мог опоздать на встречу.

В «Операции “Нефть”» я проявлял равноценный альтруизм по-разному. Во-первых, интересовался мнением OilHater’a, чем подтверждал его знания и авторитет. Во-вторых, был готов выделить свое время на личную встречу с целью решить нашу общую проблему. Все это позволило сформировать доверие и раппорт, в результате OilHater принял опасное для себя решение.

Управление ожиданиями

Все описанные выше принципы будут открывать перед вами двери, которые вы раньше считали надежно закрытыми. Это похоже на то, как если бы вы вдруг научились читать мысли или стали джедаем. Только заведете разговор — а человек уже будет готов поведать историю своей жизни. Сложнее всего будет не использовать эти навыки каждый день и просто отключать их иногда. А еще, возможно, вам будет трудно справиться с тем объемом информации о людях, который вы вдруг начнете получать.

Самую важную роль этот принцип сыграет в момент атаки. Не только объекты воздействия, но и вы сами ощутите силу валидации, доверия и раппорта, потому что в вашем теле точно так же, как и у них, будут выделяться дофамин и окситоцин. Химия для всех работает одинаково, за приятные ощущения отвечают одни и те же вещества, так что, возможно, на пике этой радости вам захочется пойти на неоправданный риск. Но если вы будете продвигаться слишком быстро и заходить слишком далеко, это может разрушить раппорт — и, скорее всего, восстановить его будет невозможно.

Однако у этой медали есть и обратная сторона. Вам придется контролировать свои ожидания и в ситуации, когда все пойдет не так, как вам хочется. Рекомендую соблюдать правило: «После общения с вами человек должен почувствовать себя лучше, чем до него». Если заметите, что ваши попытки установить раппорт безуспешны или, тем более, вызывают неприятные эмоции, лучше отступите. Найдите повод для того, чтобы уйти и придумать другой план атаки. Не стоит портить профессиональную репутацию только потому, что доказать свою правоту вам было важнее, чем решить задачи клиента.

Эти принципы настолько эффективны, что у вас наверняка возникнет желание применять их и в повседневной жизни. Будет большой соблазн превратить других людей в инструменты достижения собственных целей. Что же, в этом случае придется применить на практике управление ожиданиями и контролировать свое желание использовать эти принципы за пределами пентестов и «отключать» эти навыки в повседневном общении.

В ходе «Операции “Нефть”» мне часто приходилось умерять свой пыл. Например, надо было ждать больше двух недель, пока OilHater заметит меня и ответит на одном из форумов. Кроме того, он часто пропадал и мне приходилось ставить себя на место «Пола»: как бы он отреагировал на это. И каждый раз я не знал — пропал ли OilHater насовсем или только на несколько дней. Но управление ожиданиями и терпение позволили мне добиться своего.

Машина по производству раппорта

Когда мы с учениками обсуждаем тему установления раппорта, меня часто спрашивают: как отработать необходимые навыки еще до становления профессиональным социальным инженером (ну, например, в процессе профессиональной подготовки)? Чтобы на реальном задании все, как говорится, от зубов отскакивало. В этом разделе я собрал советы, которые пригодятся для отработки и оттачивания практического применения этих 10 принципов.

Друзья и родственники

Не нужно ждать начала рабочего дня, чтобы потренироваться. Выберите один из принципов (например, валидацию) и попробуйте попрактиковать его на ближайшем семейном мероприятии. Понаблюдайте за двоюродной сестрой, с которой давно не виделись, а потом скажите в ее адрес искренний комплимент. Задайте ей личный вопрос и внимательно выслушайте ответ. Обратите внимание на то, насколько охотно она будет говорить.

На следующей встрече выберите другой принцип (например, использование невербальных сигналов) и обратите внимание на то, как

меняется реакция людей в зависимости от перемены вашей позы в ходе разговора. Со временем вы наработаете собственный набор инструментов и поймете, что эффективно и не эффективно лично для вас. Вскоре вы научитесь использовать принципы автоматически.

Чтение

Читайте книги о раппорте (например, Робина Дрейке). Подробный список можно найти на https://www.social-engineer.org/resources/seorg-book-list/. Изучение этих принципов в теории позволяет закрепить знания, чтобы их было проще применить на практике.

Подробно разбирайте неудачи

Когда ситуация развивается не по плану и общение не ладится, не пытайтесь спрятаться от неудачного опыта и поскорее его забыть. Гораздо полезнее поступить наоборот: разложить произошедшее по полочкам и постараться определить причины провала.

Лично мне на неудачах учиться проще, чем на успехах. Да и успехи приобретают большее значение благодаря неудачам. Привычка анализировать неудачи и извлекать из них уроки помогает мне быть лучшим учителем и эффективнее справляться с профессиональными задачами в роли специалиста по проверке безопасности.

Резюме

В этой главе мы разобрали, что такое раппорт, как его устанавливать и использовать в своих интересах. Связанные с этим процессом навыки помогают повысить эффективность общения, они очень важны для тех, кто собирается стать социальным инженером.

Не важно, какие средства вы планируете использовать в работе (фишинг, вишинг, СМС или личное взаимодействие), эти навыки помогут добиться максимальных результатов. И хочу подчеркнуть еще раз: учиться расставаться с людьми, не разрушая раппорт, так же важно, как и учиться его устанавливать.

Я часто замечал, что в процессе обучения вышеописанным принципам расставание с объектом дается сложнее всего. Главная причина — в том, что интуитивно это кажется чем-то плохим. Человек только что рассказал вам историю своей жизни, дал массу информации по делу и еще больше — не по делу, а вы в ответ просто поворачиваетесь и уходите?

Конечно, нет. Расставаться нужно красиво. Следуя всем 10 принципам, сделать это несложно. Сейчас я приведу несколько примеров.

Вот первая ситуация. Можно искусственно ограничить время взаимодействия. Я могу посмотреть на часы и сказать: «О боже, как быстро время пролетело! С вами было так интересно беседовать, что я совсем перестал смотреть на часы [валидация]. Очень жаль, но мне пора бежать [усмирение эго]».

Если для установления раппорта вы выбрали взаимовыгодный обмен и валидацию, можете сказать: «Только подумайте! Меня так увлек разговор с вами [еще больше валидации], что я совсем забыл: жена/муж просил(а) меня купить салат по дороге домой. Лучше мне поторопиться [снова равнозначный обмен: объект сообщил вам личную информацию, и вы «поделились» с ним рассказом о супруге и ваших планах на ужин]!»

Обычно я заранее продумываю несколько стратегий выхода из общения с учетом конкретной легенды. Так проще найти валидирующие и добрые формы поведения, которые позволят расстаться с человеком, не разрушая раппорт.

ПРЕДОСТЕРЕЖЕНИЕ Используя техники установления раппорта в закрытой среде (например, в самолете, поезде или общественном транспорте), нужно отдавать себе отчет в том, что возможности прекратить общение и уйти у вас будут ограниченны. Например, при использовании этих принципов во время перелета я рекомендую сразу ориентировать собеседника на временно́е ограничение. Например: «Я собирался немного поспать, потому что мне придется поработать на свежую голову сразу после приземления. Но сначала я хотел поинтересоваться: откуда вы?» Я тем самым сообщал человеку, что не настроен на длительное взаимодействие. Впрочем, слишком часто такой заход не давал желаемого эффекта и я ввязывался в трехчасовое (а однажды, не поверите, девятичасовое!) общение. Какое там поспать! Поэтому теперь я просто надеваю наушники и стараюсь не встречаться глазами с теми, с кем не хочу говорить.

Раппорт — это связь между вами и другими людьми. Выстраивая ее, вы каждый раз выбираете, каким образом себя вести, чтобы собеседник почувствовал себя лучше или хуже после общения с вами. И каждый раз в результате вы сталкиваетесь с возможностью повлиять на человека, с которым говорите, и даже как-то им манипулировать. Об этом мы и поговорим в следующей главе.

6 Сила влияния

Тайна моего влияния заключается в том, что оно всегда оставалось тайным.

Сальвадор Дали

В этой главе мы будем говорить как о влиянии, так и о манипуляции, но сначала я хочу сосредоточиться именно на влиянии. Что это вообще такое? Давайте определимся для начала.

Я трактую это понятие следующим образом: «Влияние позволяет заставить другого человека захотеть сделать то, что вам от него нужно». То есть у человека должна возникнуть мысль о том, что нужно совершить некое действие а оно впоследствии окажется вам на руку. Но ваш визави должен запомнить это действие так, словно он сам решил его сделать. Потому что собственные идеи кажутся нам самыми замечательными на свете и мы готовы вкладывать в их реализацию массу сил.

Один из ведущих специалистов в этой теме — Роберт Чалдини. Он посвятил изучению силы влияния не одно десятилетие: исследовал его, писал о нем, занимался совершенствованием искусства влияния. В 86-м выпуске СИ-подкаста мне выпала честь лично беседовать с Бобом после того, как он сам изъявил желание поучаствовать в нашем шоу. Тогда и состоялась одна из самых увлекательных бесед в моей жизни, из которой я вынес для себя очень много нового.

В 1984 году Боб написал книгу «Психология влияния», которой я пользуюсь и по сей день. В ней описаны шесть принципов влияния, которым без труда можно дать определение, им легко обучить, их просто отследить. Из практических соображений я взял на себя смелость дополнить эти шесть основополагающих принципов двумя дополнительными.

В этой главе я сначала раскрою смысл каждого из них в контексте исследований и работ великих ученых вроде самого доктора Чалдини. А затем рассмотрю каждый из них с позиции социального инженера.

Затем расскажу о фрейминге — явлении, непосредственно связанном с влиянием (если коротко, фрейминг можно считать основой, на которой выстраиваются ваши убеждения, точки зрения, мысли). Затем мы обсудим способы влияния на фреймы объектов воздействия. Мы также поговорим о манипуляции — злой «сестре» влияния. А затем, подводя итоги, я дам несколько полезных советов, которые помогут применять этот навык.

УРОК ПО ФОРМИРОВАНИЮ НАВЫКА

За годы работы в области СИ мне не раз доводилось применять свои навыки, чтобы остановить людей, представляющих опасность для детей. Расскажу об одном таком задании, чтобы вы поняли, почему в моем определении влияние звучит именно так, а не иначе.

Для операции «Аренда машины», про которую я сейчас расскажу, нам нужно было выведать домашний адрес человека, который, как мы знали, торговал детьми. Правоохранительные органы уже нашли доказательства его вины, но он так часто и хаотично передвигался, что определить его домашний адрес не удавалось. Мы знали, что он отправился в некий город и взял там напрокат машину. В наши задачи входило найти компанию, услугами которой он воспользовался, и уговорить ее сотрудника сообщить нам домашний адрес преступника.

Я использовал легенду владельца местной пиццерии: сказал, что нашел в своем ресторане iPad, который забыл один из клиентов, но поскольку гаджет был заблокирован, я не мог вернуть его хозяину. Как известно, сотрудники компаний по прокату машин не рвутся сообщать кому ни попадя адреса своих клиентов. Поэтому я собирался пообещать бесплатный обед в своем ресторане сотруднику, который предложит стоящую идею о том, как найти владельца устройства.

Пришлось немного попотеть, но в конце концов я выяснил, в какой именно компании была арендована машина. Ниже я привожу часть диалога с ее представителем.

ОБРАТИТЕ ВНИМАНИЕ В целях безопасности все имена и названия в этой истории были изменены.

Я: Слушайте, я не знаю, что делать. Готов предложить бесплатную пиццу за дельное предложение о том, как найти владельца.

Сотрудник: Правда? Вообще-то я очень люблю пиццерию «У Тони»! Как я могу вам помочь?

Я: Я бы отправил забытый iPad владельцу напрямую, но у меня нет его адреса. А давайте я отдам этот гаджет вам и вы сами займетесь розысками хозяина?

Сотрудник: Тони, мне очень жаль, но я правда не могу этого сделать. У нас есть строгие требования относительно передачи вещей, которые были найдены не в наших автомобилях.

Я: Да, понимаю. Черт, ну как мне теперь быть? Может, подскажете, как можно узнать домашний адрес этого человека?

Сотрудник [несколько секунд раздумывает, а потом шепчет]: Знаете, вообще-то я не должен этого делать, но вам я помогу. Сейчас скажу, где он живет, у нас есть эта информация.

Я: Стив, это гениально! Как я сам не догадался, что он должен быть у вас в базе? Спасибо! Как и обещал, вас ждет купон на $25 в моей пиццерии!

Обратите внимание: в ходе этого диалога я дважды проталкивал идею о том, чтобы сотрудник компании дал мне адрес, но затем разыгрывал дурачка вместо того, чтобы попросить напрямую. Это — отличный пример использования принципов влияния и одновременного внедрения объекту мысли о том, чтобы он сообщил мне нужную информацию. В итоге молодому человеку показалось, что это его идея, а значит, решить мою задачу стало проще.

По ходу главы вы, возможно, заметите много пересечений с принципами установления раппорта.

ОБРАТИТЕ ВНИМАНИЕ Я основал некоммерческий фонд Innocent Lives Foundation («Невинные жизни», https://www.innocentlivesfoundation.org/), работа которого направлена на защиту детей от взрослых с недобрыми намерениями. В работе фонда участвуют специалисты по

информационной безопасности, которые тесно сотрудничают с представителями органов правопорядка. Это делается для достижения общей цели: поиска злодеев, использующих интернет для эксплуатации детей. Описанные в этой главе навыки всегда помогают нам в этой работе.

Первый принцип: взаимный обмен

Взаимный обмен во многом похож на принцип равноценного альтруизма при установлении раппорта. Он основан на том, что большинство людей стремятся оказать встречную услугу тем, кто был к ним добр или дал им что-то нужное. Но даже если эта вещь нам не нужна, наш мозг, согласно Чалдини, не успокоится, пока мы не отплатим чем-то дарителю. Маркетологи этот принцип знают и постоянно его используют.

Взаимный обмен на практике

Вспомните ситуацию, когда в супермаркете вам предлагали попробовать образец какого-то товара. Магазины и маркетинговые компании, организующие подобные раздачи, прекрасно знают, что большинство людей покупает продукт после получения бесплатного пробника.

Исходя из тех же побуждений, люди охотнее согласятся выполнить указание или просьбу человека, который за что-то их похвалил.

Однажды я вместе с женой и дочкой улетал домой из Лондона, где находился по работе. Мы купили премиум-билеты в эконом-класс, чтобы добраться домой с относительным комфортом. А путешественники мы правильные, поэтому прибыли в аэропорт за три часа до посадки.

Я толкал тележку с чемоданами, которые, мягко говоря, были перегружены. Практически на подходе к стойке регистрации я наехал колесом на какую-то неровность, и весь наш багаж с грохотом полетели на пол. Я улыбнулся и пошутил: «Столкновение на шоссе М5».

Окружавших нас британцев повеселило, что американец (а по моему акценту это очевидно) использовал в шутке название местной дороги. Сотрудница авиакомпании тоже улыбнулась и пригласила зарегистрироваться на рейс. Я полез за паспортами, а жена рассыпалась в комплиментах прекрасному шарфу, который женщина элегантно повязала на шею.

Прошу заметить: моя жена — не социальный инженер. Она просто по природе своей замечательная женщина, которая искренне любит людей. Так что она не лукавит, когда говорит: «Вы просто идеально накрашены!» или «Мне так нравится, как этот шарфик подчеркивает цвет ваших глаз!».

Наблюдая за взаимодействием моей жены и сотрудницы авиакомпании, я заметил невербальные сигналы второй, указывающие на то, что она

испытывает гордость и радость, а значит, ее мозг фонтанировал теми химическими веществами, которые делают нас счастливыми. И тут я подумал: «Крис, пришло твое время, действуй, проси!»

Передав женщине наши паспорта, я приобнял жену и сказал: «Мы с женой хотели спросить, сколько стоит поменять наши билеты на первый класс?»

И сейчас я не преувеличиваю: женщина начала быстро стучать пальцами по клавиатуре и несколько минут спустя выдала нам три посадочных талона в первый класс — без дополнительных комиссий, зато с доступом в VIP-лаундж на ближайшие три часа ожидания.

Только подумайте: пара комплиментов плюс добрая шутка — и принцип взаимного обмена сработал нам на руку!

На илл. 6.1 этот принцип изображен схематически.

Принцип взаимного обмена работает, только когда вы последовательно соблюдаете все перечисленные шаги. Нельзя озвучивать запрос или указание слишком рано. Делать это можно только после того, как у объекта воздействия сформируется чувство долга. Потому что именно это чувство существенно увеличивает шансы на удовлетворение вашего запроса.

Илл. 6.1. Взаимный обмен на практике

Взаимный обмен в работе социального инженера

У вас наверняка уже возникло пять миллионов идей о том, как использовать принцип взаимного обмена в социальной инженерии. Но хочу сразу дать вам важную подсказку: сложность запроса должна соответствовать ценности вашего подарка с точки зрения получившего его человека.

Подумайте немного над этой информацией. Вспомните слова Чалдини о том, что человек почувствует потребность вернуть долг вне зависимости от того, хотел он получить что-то от вас или нет. Если же реципиент воспримет ваш дар как нечто для себя ценное, его желание вернуть долг или даже превысить вашу щедрость будет еще сильнее.

Я вхожу в небольшой клуб хакеров, которые по совместительству являются еще и большими ценителями виски. Собираясь вместе, мы часто обмениваемся бутылками этого замечательного напитка. Каждый приносит что-то для других, и каждый возвращается домой с подарками. Обычно мы заранее оглашаем определенные ограничения, чтобы не получилось: один принесет «дар» ценою в $200, а другой — что-то намного более эксклюзивное и дорогое. То есть мы сами контролируем обмен, чтобы никому не пришлось чувствовать себя обязанным.

Социальному инженеру обязательно нужно заранее узнать, что ценит объект воздействия и что считается ценным в компании. И легенду нужно выбирать, учитывая этот фактор. Если вы предложите человеку что-то действительно для него ценное, то с большей вероятностью достигнете цели.

Например, в ходе операции «Аренда машины» мне не составило труда узнать, что объект любит посещать пиццерию «У Тони». Поэтому я и предложил ему пиццу за толковую идею решения моей проблемы. Но! Я не говорил: «Если вы сообщите мне адрес вашего клиента, я дам вам пиццу». Почему?

Объяснение простое: между нами на тот момент еще не возник раппорт. Просьба о такой серьезной услуге (разглашении личных данных клиента) до установления раппорта сразу насторожила бы сотрудника службы аренды.

А я предложил ему бесплатную еду, а потом намекнул на то, что мне нужно, — и в результате объект сам «придумал» решение, которого я от него и добивался.

ЗАНИМАТЕЛЬНЫЙ ФАКТ

Мне не хотелось, чтобы парень из компании по аренде автомобилей пришел в пиццерию «У Тони» и получил от ворот поворот. Так что, закончив беседу с ним, я позвонил в ресторан и купил сертификат на $25 на имя этого молодого человека с пометкой «От Тони».

А вот еще один пример ситуации, в которой я воспользовался этим принципом. Мне нужно было организовать адресный фишинг. Объектом атаки был генеральный директор одной компании, который, как выяснилось из открытых источников, страстно увлекался бегом и был марафонцем. Я выяснил это, потому что нашел огромное количество селфи, которые он публиковал, когда бежал очередной марафон.

Поэтому для атаки я выбрал легенду представителя компании, отвечавшей за маркетинговое сопровождение марафона. Сообщение

было примерно таким: «В ходе последнего марафона “Бежим для детей”, в котором вы приняли участие, было сделано несколько ваших фотографий. Мы хотели бы использовать их в будущей промокампании. Пожалуйста, перейдите по ссылке ниже, чтобы посмотреть фотографии, и сообщите, даете ли вы согласие на их использование». Если мне не изменяет память, гендиректор перешел по ссылке меньше чем через час после получения письма.

Постарайтесь узнать, что для человека действительно важно, — и он примет ваше предложение не задумываясь.

Второй принцип: обязательства

Может показаться, что обязательства — это почти то же самое, что и взаимный обмен. Однако разница между этими понятиями все же есть. Если взаимный обмен основывается на чувстве долга, возникшем в результате получения какого-то подарка или услуги от вас, то обязательства основаны на том же чувстве долга, проистекающем, однако, из другого источника: социальных норм и ожиданий.

Обязательства на практике

Своим ученикам со всего мира я задаю один и тот же вопрос: представьте, что вы стоите в пробке и тут перед вами вклинивается машина. Как думаете, что водитель должен сделать после этого?

Обычно предлагают следующие варианты: помахать, поднять руку, кивнуть. Все эти жесты имеют одинаковый смысл: вклинившийся водитель должен (обязан) проявить к вам уважение и благодарность за вашу доброту. А что произойдет, если он этого не сделает?

Как-то раз я ехал на встречу в Вашингтон по четырехполосному шоссе. Но на одном участке из-за ДТП всем машинам нужно было перестроиться в одну полосу. Образовалась медленно ползущая змейка. Я подумал, что не стоит позволять такой глупости испортить себе день: включил музыку и стал ползти вместе со всеми. Но были и желающие всех опередить — они проезжали далеко вперед по обочине, а потом пытались протиснуться в ряд перед кем-нибудь. Другие водители особого альтруизма к ним не проявляли и старались не пропускать. Ну а я притормозил и моргнул поворотниками, пропуская водителя, который пытался встроиться передо мной.

Он воспользовался моим приглашением и какое-то время ехал передо мной. Но сколько я ни всматривался, не увидел ни благодарного кивка с его стороны, ни даже приветливого взмаха руки. И тут я почувствовал, как моя кровь закипает: лицо покраснело, я стал вести машину намного агрессивнее. «Правильно тебя никто не пропускал», — злобно думал я,

словно у других водителей было шестое чувство, позволившее заранее понять, что этот водитель не оценит доброго поступка.

У меня в голове проносились гневные тирады по поводу того, как тот хам не достоин дышать воздухом и топтать землю. Позже, когда пробка рассосалась и впереди замаячили четыре свободные полосы, я только и думал о том, как вдавлю педаль газа в пол и обгоню этого грубияна — одним словом, покажу, кто хозяин этой дороги.

Сказано — сделано: я ударил по газам, и мой шестицилиндровый супернавороченный спорткар рванул вперед. Когда я поравнялся с машиной невежливого водителя, то не смог удержаться и заглянул к нему в окно. И тут я увидел, что у этого человека… нет одной руки. Мой гнев за долю секунды превратился в смирение. Я улыбнулся и помахал водителю.

Зачем я делюсь этой историей позора? Чтобы показать, какую ярость ощущает человек, которому кажется, будто другой не выполняет своих обязательств перед ним. Лишь когда я узнал, что у водителя была более чем уважительная причина не посылать мне благодарственных жестов, я понял, как ошибся в своих суждениях.

Вспомните об этом, когда в следующий раз будете разговаривать с кем-нибудь. Скажем, вам зададут хороший вопрос — а вы проигнорируйте его, не отвечайте. Просто смотрите на человека как ни в чем не бывало. Вас наверняка спросят, все ли с вами в порядке — а вы скажите «Ага»… и все равно не отвечайте.

Обязательства имеют для нас огромное значение, особенно когда речь заходит о социальных нормах. Круг обязательств схематически изображен на илл. 6.2.

Как социальный инженер, вы должны учитывать ожидаемые реакции и обыгрывать их. Если же вы этого не сделаете, то снизите собственные шансы на установление раппорта, потому что объект задумается о причинах вашего «ненормального» поведения.

Илл. 6.2. Обязательства в действии

Обязательства в работе социального инженера

Социальные инженеры постоянно моделируют ситуации, в которых объект воздействия чувствует себя обязанным поступить определенным образом. Например, не придержать дверь перед женщиной или любым человеком с тяжелой ношей считается грубостью — и специалист в области СИ может использовать эту норму этикета в своих интересах.

На одно из заданий я взял с собой коробку с телефонами и компьютерными запчастями. Затем дождался, когда после обеда на входе соберется народ, и направился к двери. Моей задачей было пройти в здание без пропуска. Я еще даже не успел приблизиться к входу, как какой-то добрый человек пригласил меня жестом: «Я подержу вам дверь!»

— Надо было сначала проверить, есть ли у него пропуск, — негромко сказал его коллега.

— Полностью согласен. Я не удержу эту коробку одной рукой, а пропуск лежит у меня в переднем кармане. Проверьте, если хотите, — не растерялся я и повернулся к недоверчивому мужчине бедром так, чтобы карман, где якобы лежал пропуск, оказался к нему ближе.

— Э нет, я к вам в штаны не полезу, — отмахнулся он.

— Конечно, что это я, простите! Тогда подержите, пожалуйста, эту 20-килограммовую коробку, я его сам достану.

— Да проходите уже, заняться мне больше нечем, как проверять ваш пропуск, — буркнул мужчина и пошел по своим делам.

Вежливый человек обязан подержать дверь перед тем, кто идет с тяжелой ношей. И я «отплатил» за эту услугу готовностью из ответного чувства долга вывернуть свои карманы. Но лезть ко мне в штаны не

захотелось даже недоверчивому сотруднику, так что я проник в здание без пропуска.

И такой сценарий помогал мне не раз. Но однажды случилась осечка. Одна из сотрудниц компании, к моему удивлению, ответила: «В каком кармане? В этом?» — и потянулась за пропуском.

Я попытался выйти из ситуации, сделав ее еще более неловкой: «Вообще-то я не помню точно, в каком именно. Попробуйте оба». Я надеялся, что ее это остановит. Но нет! Она спокойно запустила руку мне в карман — и тут уже неловко стало мне!

Не найдя в одном кармане ничего, кроме ключей, она сказала: «Так, тут нет. Давайте другой!» Но и там лежали только нож и портмоне. Она внимательно посмотрела на меня и спросила: «Может, в бумажник положили?»

Я ответил: «Да, наверное», хотя, конечно же, знал, что и там она ничего не найдет. Женщина открыла бумажник и увидела младенческую фотографию моей дочки. «Какая милашка! Как ее зовут?» — тут же спросила она.

Мы еще 15 минут говорили о моей семье (и все это время она держала мой кошелек, нож и ключи, а я не выпускал из рук дурацкую тяжеленную коробку). Потом она разложила все мои вещи обратно по карманам и заботливо сказала: «Вам стоило бы сообщить о том, что потеряли пропуск, а то накликаете неприятности. Увидимся в офисе!» На этой благостной ноте мы и расстались. Между нами установился раппорт и дружеская связь, поэтому женщина почувствовала себя в некотором смысле обязанной мне доверять.

Так что, дорогой читатель, запомните: обязательство — мощный принцип социального взаимодействия, способный существенным образом облегчить жизнь социального инженера.

Третий принцип: уступки

Оксфордский словарь английского языка дает следующее определение глаголу «уступать»: «Признавать или соглашаться с истинностью чего-либо после противостояния или отрицания этого».

Само определение влияния предполагает, что, если человек считает идею своей, она наверняка будет казаться ему отличной. И именно уступки помогают внушить объекту воздействия мысль, что совершить нужное вам действие — это «его идея».

Уступки на практике

Там, где я живу, Американское общество по предотвращению жестокого обращения с животными, используя уступки, весьма успешно

подталкивает людей вносить пожертвования. Происходит это обычно по следующему сценарию.

Звонит телефон. В трубке — женский голос: Доброе утро, мистер Хэднеги. Меня зовут Керри, я представляю людей, неравнодушных к судьбе животных Монтроуза. Как поживает ваша собака?

Я [отвечая, я понимаю: этим вопросом она заставляет меня почувствовать, что проблема касается и меня; начинаю улыбаться и думаю: «Боже, как же остановиться»]: У нее все прекрасно. Хотя годы, конечно, идут.

Женщина: Очень рада слышать, что у нее все в порядке. И приятно разговаривать с человеком, который тоже неравнодушен к животным. Сегодня нам всем нужно объединить усилия, поэтому мы и просим вас о помощи. Как вы наверняка знаете, наша организация занимается спасением бездомных животных в нашем регионе. Мы хотим, чтобы для каждого животного нашелся дом и такой же любящий хозяин, как и у вашей собаки. Скажите, можете ли вы помочь нам в этом деле?

Я [уже чувствую приближение главного вопроса]: Ну, животных-то я действительно люблю. Как вы предлагаете вам помочь?

Женщина [говорит четко и решительно]: Нам необходима финансовая помощь, и многие неравнодушные люди помогают приюту, перечисляя $250 на нужды животных.

Я [чувствую себя сильным человеком, потому что могу просто взять и отказать]: $250?! Нет, извините, столько я пожертвовать не могу. Я бы с радостью, но такой суммы у меня сейчас просто нет.

Женщина: Понимаю. Сейчас в стране не самые легкие времена, и это действительно крупная сумма. Может быть, в таком случае вы хотели бы пожертвовать $25?

И я, недолго думая, тут же потянулся за кредиткой. Понимаете, что произошло? Я трижды согласился (можно сказать, уступил):

- Подтвердил, что люблю животных.
- Выразил желание помочь.
- Сказал, что помог бы, но такой суммы у меня нет.

И когда мне предложили альтернативный вариант, я уже не мог отказаться. А что бы произошло, назови представительница общества сразу $25? Скорее всего, объем перечисленных в итоге пожертвований был бы значительно меньше. Однако сразу завысив предполагаемую сумму, она обеспечила организации повышение суммы реально сделанных взносов.

Эту тактика часто используются и сотрудники правоохранительных органов. Если им удается добиться от подозреваемого случайного

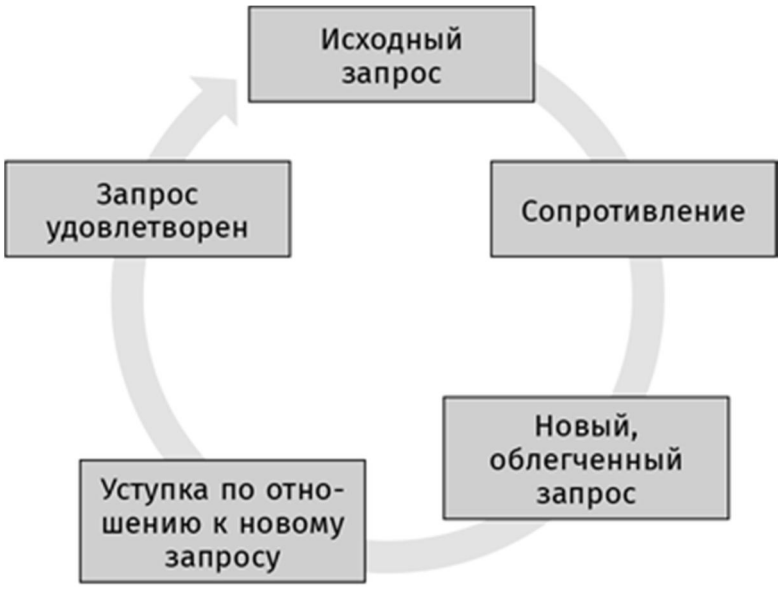
признания в каком-то маленьком проступке, позже ему уже будет невозможно отказаться от этих слов.

Давайте разберем две разные формулировки, которые мог бы использовать детектив. На вопрос: «Вы были в баре у Ли в 11 вечера, когда произошло ограбление?» — подозреваемый, скорее всего, ответит: «Нет, не был». Если же детектив спросит: «Так что вы видели в 11 часов, когда произошло ограбление в баре у Ли?», намного выше вероятность получить ответ: «Да ничего я не видел, темно же было». И все, дознаватель может заключить, что подозреваемый все-таки был в баре в указанное время. Подозреваемый уступил! Ответив на вопрос с подвохом, он, по сути, согласился с подразумеваемым утверждением о том, что находился в месте преступления.

На илл. 6.3 схематически изображен процесс уступки в диалоге.

Уступки в работе социального инженера

В ходе одного вишинга перед нами стояла задача собрать полные имена и идентификационные номера сотрудников, а также номера их социального страхования. Мы разработали две легенды, которые показались мне вполне подходящими, и начали обзванивать объекты воздействия.



Илл. 6.3. Уступки в действии

Телефонные разговоры были примерно следующего содержания:

Я: Добрый день. Это Пол из IT-отдела. Могу я услышать Сэлли Дэвис?

Объект: Это я. Чем могу быть вам полезна, Пол?

Я: Вчера мы прошивали корпоративный BIOS под систему RFID-пропусков, и в процессе некоторые данные оказались утеряны. Скажите, не было ли у вас сегодня утром проблем с пропуском?

Объект: Да нет, все работало как обычно.

Я: Ага, просто замечательно. Значит, вам повезло. У многих пользователей, которых коснулась эта проблема, возникли трудности на КПП. Тем не менее мне нужно проверить данные вашего аккаунта, чтобы у вас и в будущем не было проблем. Это займет не больше минуты.

Объект: Ладно. Какая информация вам нужна?

Я: Ваше полное имя, идентификационный номер сотрудника и номер социального страхования.

Объект: Эммм… вообще-то такую информацию разглашать не рекомендуется. Напомните, пожалуйста, ваше имя. Я проверю.

Разумеется, продолжения у этого разговора не было. Подобный тупиковый сценарий повторялся снова и снова — казалось бы, эпический провал. Тогда я решил сделать паузу, чтобы спокойно поразмышлять о принципах влияния, а затем внес в легенду всего одно изменение. Приведенный ниже разговор продолжался сразу после того, как объект воздействия сообщал мне, что утром без проблем прошел КПП.

Объект: Проблем не было, пропуск сработал, я прошел на работу как обычно.

Я: Ага, просто замечательно. Значит, вам повезло. У многих пользователей, которых коснулась эта проблема, возникли трудности на КПП. Тем не менее мне нужно проверить данные вашего аккаунта, чтобы и в будущем у вас не было пробоем. Это займет не больше минуты.

Объект: Ладно. Какая информация вам нужна?

Я: Нужно проверить, правильно ли написано ваше имя. В базе записано С-Э-Л-Л-И, верно?

Объект: Нет, здесь ошибка. Мое имя пишется через «А», а не через «Э».

Я: О, значит, все-таки не зря я вам позвонил. Тогда продиктуйте, пожалуйста, по буквам, как пишется ваша фамилия.

После этого я спрашивал, в каком отделении объект воздействия работал, проверял электронный адрес — и к моменту, когда мы добирались до идентификационного номера сотрудника и номера социального страхования, человек, уже сделавший столько уступок, соглашался рассказать и это. После изменения легенды в среднем 84% звонков заканчивались успехом.

Социальному инженеру не стоит торопиться в процессе сбора информации. Пусть объект воздействия сообщит вам сначала менее значимые данные, а после этого у него появятся чувства, которые заставят его идти на уступки и подчиняться.

Четвертый принцип: дефицит

«Распродажа по случаю закрытия!»

«Самые низкие цены в истории!»

«На всей земле осталось всего 10 экземпляров!»

Почему такие слоганы помогают продавать? Субъективная ценность предмета, который кажется нам дефицитным или недоступным, быстро растет. Например, насколько ценен для нас один кекс из упаковки, где их целых 20? И как изменится его субъективная ценность, если окажется, что остальные 19 кексов уже съедены?

Дефицит на практике

Пока мы готовились к одной из конференций DEF CON, я придумал новые нюансы социально-инженерной игры «Захват флага». Детям нужно было решать загадки. Выигравший подходил к большой коробке в дальнем конце комнаты и просовывал в нее трубку. В коробке сидел «снайпер» с игрушечным автоматом и стрелял в остальных игроков через трубку мягкими пульками. Тот, в кого он попадал, должен был выйти из комнаты и начать заново.

ЗАНИМАТЕЛЬНЫЙ ФАКТ

Соревнование прошло на ура. А если вам захочется узнать, как вышло, что победила команда детей, уделав даже нас, взрослых, то вам придется спрашивать меня об этом лично.

В качестве оружия я выбрал игрушечный автомат модели Nerf CS6 Long Shot. Вскоре компания Nerf объявила о прекращении производства этой игрушки. А пришедшая на смену ей новая модель многим показалась хуже.

Дома у меня такая игрушка была, и вторая в хозяйстве вряд ли пригодилась бы, так что я решил продать ее на eBay за $99 — без наценки, по той же цене, что недавно купил. В первый день предложенная цена за нее достигла $199, потом 250, потом 299, потом 340. Под конец торгов она поднялась до $410! Еще раз: $410 за пластиковую игрушку, которая стреляет мягкими пульками на расстояние до 15 метров! (Конечно, у нее есть оптический прицел и четыре съемные насадки — но все же…)

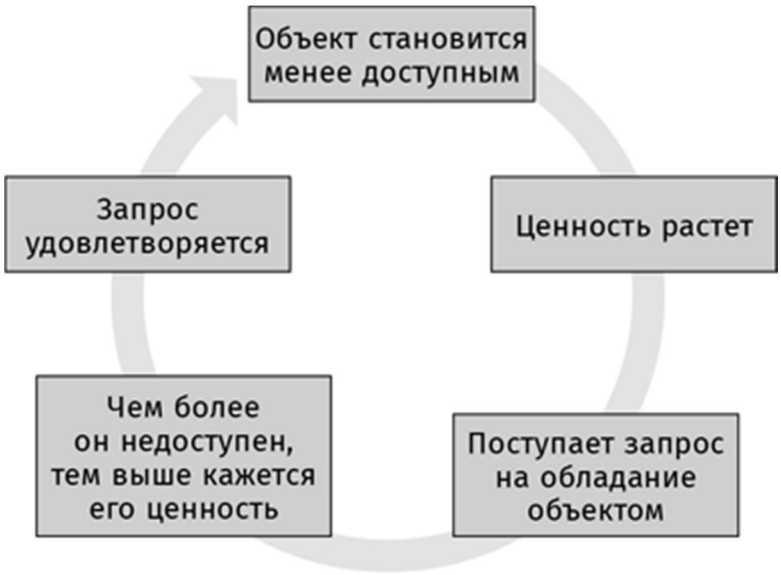
Да за $410 можно купить настоящее оружие! Что же может заставить человека выложить столько денег за кусок пластика? Дефицит. Эта модель больше не выпускалась, а потому стала уникальной и ее ценность взлетела до небес.

Многие компании используют ограничение товаров, еды, лекарств, времени, драгоценностей — да чего угодно! — для повышения стоимости своего продукта в глазах покупателя. На илл. 6.4 изображен континуум дефицита.

Дефицит в работе социального инженера

В ходе одной операции мы проводили сбор данных из открытых источников о гендиректоре компании. Он рассказывал в соцсетях о том, как провел свой первый за три года отпуск: вместе с семьей отправился на Багамы. Директор опубликовал фотографии сборов, поездки в аэропорт, посадки, ожидания взлета в салоне самолета. Под одним из снимков красовалась подпись: «Наконец-то! Две недели в раю!».

Вооружившись этими знаниями, а также информацией о компании, которая осуществляла IT-поддержку его организации (ее мы получили благодаря исследованию содержания мусорных баков), я прошел через входные двери в здание и направился прямо к Джейн, вахтерше. Между нами состоялся примерно следующий диалог:



Илл. 6.4. Дефицит в действии

Джейн: Добрый день. Чем могу помочь?

Я: Здравствуйте. Меня зовут Пол, я из компании АБВ. Меня вызвал Джефф, чтобы я решил проблему с… [С умным видом листаю свои записи, словно ищу что-то конкретное.] Ага, у него тормозит компьютер. Джефф полагает, что это вирус.

Джейн [сверяется с органайзером]: Знаете, Пол, мне никакой информации об этом от Джеффа не поступало. Извините, я не могу вас впустить, вам придется вернуться позже.

Я: Честно говоря, даже не знаю, что вам сказать. Джефф позвонил мне, сообщил, что уезжает на Багамы на две недели, и потребовал, чтобы я разобрался с проблемой до его возвращения — а то он очень разозлится. Я перенес четыре встречи — специально, чтобы решить вопрос прямо сегодня. В ближайший месяц у меня свободных окон не будет. [Делаю паузу.] Хотя, может, в этом и нет ничего страшного. Я отправлю Джеффу e-mail. Напишу: из-за того, что он забыл вас предупредить, я теперь смогу разобраться с его компьютером только через четыре недели [во время этой тирады я протягиваю Джейн свои записи]. Только, пожалуйста, поставьте здесь свою подпись, так я смогу

подтвердить, что сообщил вам об отсутствии у меня свободного времени на ближайший месяц.

Джейн [задумалась, смотрит на меня]: Он ведь действительно жаловался, что компьютер в последнее время тормозит. Честно говоря, не хочется мне встречать его с новостями о том, что придется ждать еще так долго... Ладно, проходите.

Так я попал в офис гендиректора, где никто за моими дальнейшими действиями не следил. Безопасность компании была подорвана.

Вымышленный дефицит времени позволил мне создать необходимость действовать здесь и сейчас. Именно ощущение дефицита заставило Джейн думать, будто ее отказ сейчас спровоцирует возникновение еще большей проблемы в будущем. А в результате под угрозой оказалась секретная информация компании.

Социальные инженеры могут создавать у объектов воздействия страх перед нехваткой времени, информации, товаров — всего того, что вы придумаете в рамках легенды. Дефицитность вашего предложения придает ему ценность, и это позволяет влиять на решения, которые принимают объекты.

СОВЕТ ПРОФИ Меня часто спрашивают: «Скольких людей из-за вас уволили?»

Но я, будучи профессионалом, всегда подчеркиваю, что результаты моей работы должны использоваться для повышения осведомленности, а не для поисков кандидатов на увольнение. Исключение составляют случаи, когда в ходе операции вскрываются нарушения закона или сознательные попытки какого-то сотрудника навредить компании. Так что я с гордостью заявляю: людей, поверивших моим легендам, увольняют очень редко и в основном за дело.

Пятый принцип: авторитет

Мы склонны прислушиваться к мнению авторитетных людей. Например:

- Если врач в белом халате попросит вас снять штаны, вы, скорее всего, так и сделаете.
- Если родитель, учитель или начальник скажет: «Не трогайте это!», вы послушаетесь.
- Если старший по званию или командир прикажет: «Упал-отжался 20 раз!», вы уж точно сделаете, что сказано.

Всех этих людей объединяет лишь одно: вы признаёте их авторитет. Но по каким признакам он определяется? Зайдя в комнату, полную незнакомых людей, сможете ли вы понять, кто из них авторитетнее?

Посмотрите на два снимка Бена, изображенных на илл. 6.5 и 6.6. Как думаете, на каком из них Бен выглядит более авторитетным? Почему?

Скорее всего, вы скажете, что авторитетность и уверенность Бен демонстрирует на илл. 6.6. На обеих фотографиях он одет и причесан одинаково, возраст его не меняется: это один и тот же человек. Но на илл. 6.6 у него правильная осанка, сложены руки, поднят подбородок, а на лице не заметно ни единого признака страха. Все позволяет сделать вывод, что перед нами уверенный в себе человек. А уверенность в себе автоматически заставляет нас ощущать авторитетность. На самом деле, когда я предлагаю своим ученикам перечислить самые показательные, на их взгляд, признаки авторитетности, они называют уверенность, громкий голос, грудь колесом, поднятый подбородок, опрятную одежду, прямолинейность и т.п.

Как чья-то авторитетность влияет на наше поведение? Мы начинаем доверять авторитетному человеку и не требуем доказательств того, что должны ему подчиняться.

Илл. 6.5. Что вам сообщают мимика и язык тела человека на этой фотографии?

Илл. 6.6. По каким признакам можно сделать вывод, что он уверен в себе?

Авторитет на практике

Одно из самых известных исследований этой темы провел доктор наук Стэнли Милгрэм. Еще в 1963 году он изучал аргументы, которые приводили в собственное оправдание обвиняемые на Нюрнбергском процессе. Чаще всего преступные действия оправдывались причиной: «Я выполнял приказ». Проанализировав материалы судебного процесса, Милгрэм написал статью «Подчинение: Исследование поведения» (https://www.birdvilleschools.net/cms/lib/TX01000797/Centricity/Domain/1013/AP%20Psychology/milgram.pdf).

Стэнли Милгрэма интересовало, возможно ли исключительно силой авторитета принудить нормальных законопослушных граждан совершить потенциально вредное для других или даже смертельно опасное действие. Конечно, такие исследования всегда имеют ряд серьезных ограничений. Как вообще посчитать, сколько людей подчинились или не подчинились бы авторитетной фигуре, которая приказала им навредить другому человеку?

На предложение участвовать в исследованиях доктора Милгрэма откликнулись совершенно разные люди. Чтобы результаты эксперимента были действительно объективными, участникам сказали, что между ними в случайном порядке распределят роли учащихся и учителей, хотя на самом деле все испытуемые выполняли роль учителя.

Они наблюдали, как «учеников» привязывали к стулу и прикрепляли им на кожу электроды. Затем озвучивались инструкции: за неправильные ответы на задания они должны будут ударять «учеников» током. На самом деле никакого тока не было и «ученики» только изображали боль от ударов.

«Учителей» (испытуемых) подводили к пульту с рычажками, каждый из которых соответствовал силе тока от 15 до 450 вольт с шагом в 15 вольт. Чтобы эксперимент казался максимально реалистичным, им даже давали попробовать на себе, как ощущается удар силой в 45 вольт.

Затем мужчина в белом халате (авторитетная фигура) садился поблизости и наблюдал за тем, как «учитель» задает вопросы. После каждого неправильного ответа «ученик» должен был получать все более сильные удары током в качестве наказания.

Если «учитель» начинал противиться, понимая, как плохо «ученику» от ударов током, мужчина в халате говорил следующее:

- «Эксперимент должен продолжаться. Пожалуйста, не останавливайтесь».
- «Серьезного повреждения тканей не происходит. Пожалуйста, продолжайте».

Звучит не слишком убедительно, правда? Тем не менее, по результатам исследования, до ударов в 450 вольт дошли 65% испытуемых!

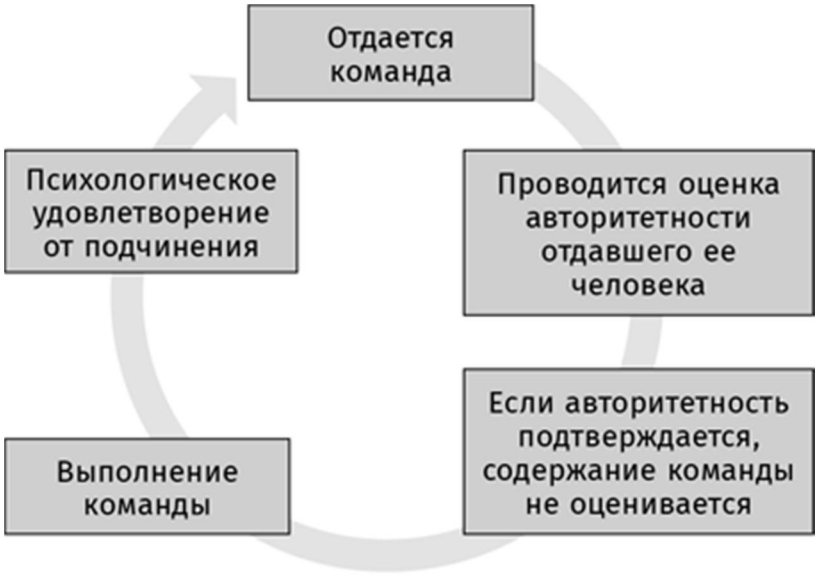
Только вдумайтесь в эти цифры. Роль учителей исполняли обычные рабочие люди. Не садисты-социопаты. Однако, как пишет Стэнли Милгрэм, 26 из 40 (65%) испытуемых продолжали увеличивать силу тока до тех пор, пока авторитетное лицо просило их об этом.

На илл. 6.7 механизм влияния авторитета изображен схематически.

Авторитет в работе социального инженера

У меня всегда возникают сложности с использованием прямого авторитета в своих легендах. В первую очередь это связано с отсутствием необходимых знаний — а значит, я рискую попасться.

Тем не менее для оказания влияния на объект воздействия бывает достаточно мнимого авторитета либо трансляции чужого авторитета. Готовясь к выполнению одного из заданий, я нашел в Сети приглашение на встречу с финансовым руководством компании, которая была целью атаки. Такую информацию вполне реально использовать в работе. Мы провели сбор данных из открытых источников по всем участникам мероприятия и выявили женщину, которая явно пользовалась авторитетом в этом коллективе. Она не просто производила такое впечатление своим поведением в социальных сетях и на популярных сайтах с рейтингами сотрудников, но также получила в нескольких отзывах статус «человека, на которого нелегко работать».



Илл. 6.7. Авторитет в действии

Тогда я сделал вот что. В списке контактов своего смартфона я изменил имя напарника на имя этой женщины (назовем ее Салли Смит), а ему сказал: «Когда увидишь, что я спорю с охранником, пришли мне такое СМС: “Где ты бродишь?! Мы уже 15 минут ждем только тебя! Немедленно приходи!”».

Взяв в руки стопку бумаг и папок, я быстро и уверенно направился в здание, всем своим видом показывая, что не собираюсь задерживаться

на посту охраны. Я знал, что меня остановят, потому что к безопасности в этой компании относились очень серьезно. Дальше ситуация развивалась следующим образом.

Охранник окликнул меня:

— Извините, сэр! Куда вы идете?! Остановитесь!

Я быстро обернулся к нему и удивленно спросил:

— Что такое? Разве вы не видели? Я буквально две минуты назад выходил отсюда, чтобы забрать из машины бумаги. Я спешу на встречу с финансовым руководством на 14-м этаже и уже опаздываю!

— Извините, сэр, но я не видел, как вы выходили из здания. Пожалуйста, покажите пропуск, — попросил охранник слегка смущенным тоном.

Я тяжело вздохнул:

— Ладно. Но когда я буду объяснять, почему заставил всех ждать, то скажу, кто именно меня не пускал.

Я порылся в карманах, по понятным причинам не отыскал в них пропуск и сказал:

— Не знаю, где он. Наверное, я оставил его…

И тут на мой телефон пришло СМС-сообщение.

Я прочитал его и показал охраннику. На экране красовалось грозное имя отправителя, Салли Смит, а под ним — сообщение: «Где ты бродишь?! Мы уже 15 минут ждем только тебя! Немедленно приходи!»

Я сказал:

— Вот сами позвоните ей и объясните, почему руководство должно сидеть и ждать эти документы. Или же мне позвонить ей и назвать имя охранника, который не давал мне пройти?!

Охранник прочитал СМС, посмотрел на меня и сконфуженно сказал:

— Простите, сэр, я правда не видел, как вы выходили из здания. Может, просто забудем это досадное недоразумение и я вас пропущу?

— Ладно, ладно — только не задерживайте меня еще дольше!

Чужой авторитет, который я всего лишь транслировал, заставил охранника совершить действие, которое точно было не в его интересах. Потому что авторитет — отличный мотиватор!

Шестой принцип: последовательность

Нам всем хочется казаться последовательными — чтобы наши слова не противоречили действиям. Это особенно заметно, когда мы начинаем отстаивать сказанное. Вспомните, как маленькие дети упорствуют в том, что, как вы знаете, правдой не является («Нет, это не я сломал лампу!»)? Ребенок ответил так на первый вопрос о том, кто виноват, и будет

придерживаться этой линии даже после того, как вы предоставите ему неопровержимые доказательства обратного.

Почему же нам так важно быть последовательными? Все просто: последовательность считается признаком уверенности и силы, поэтому мы так нуждаемся в ней.

Последовательность в действии

Я живу в тихой сельской местности, но недавно здесь обнаружили нефтегазовое месторождение. По всей стране сейчас что-то выкапывают и выкачивают, вот и по нашей деревенской дороге стали то и дело проезжать грузовики с тяжелым оборудованием.

Я не раз видел, как водители этих многотонных машин несутся со скоростью 80–100 км/ч. Это не просто безответственно, но и опасно. Некоторые из моих соседей даже установили на видных местах самодельные дорожные знаки, напоминающие водителям о необходимости соблюдать скоростной режим там, где живут дети. Но если бы какой-то сосед позвонил и попросил установить такой знак на моем участке — и тот заслонил бы мне вид из окна на цветы или на мою клевую машину, — я бы отказался. Даже несмотря на то, что лихачам на дорогах я совсем не рад.

В 1966 году исследователи Джонатан Фридман и Скотт Фрейзер, изучавшие тему последовательности в поведении человека, написали статью под названием «Подчинение без давления: Техника “Нога в двери”» (Journal of Personality and Social Psychology, сентябрь 1966, https://www.researchgate.net/publication/17217362_Compliance_Without_Pressure_The_Foot-in-the-Door_Technique). Они ходили по частным домам и просили хозяев установить на своих участках дорожные знаки, напоминающие водителям о необходимости соблюдать ПДД. Многим эти знаки испортили бы вид из окна. Отказали 83% хозяев.

Затем Фридман и Фрейзер слегка подкорректировали свое предложение — и процент согласившихся на установку знака подскочил до 76%! Согласитесь: 76% — это существенная разница! Что же изменилось? Исследователи улучшили дизайн знаков? Предложили плату за их установку? Просили сдать землю под знак в аренду?

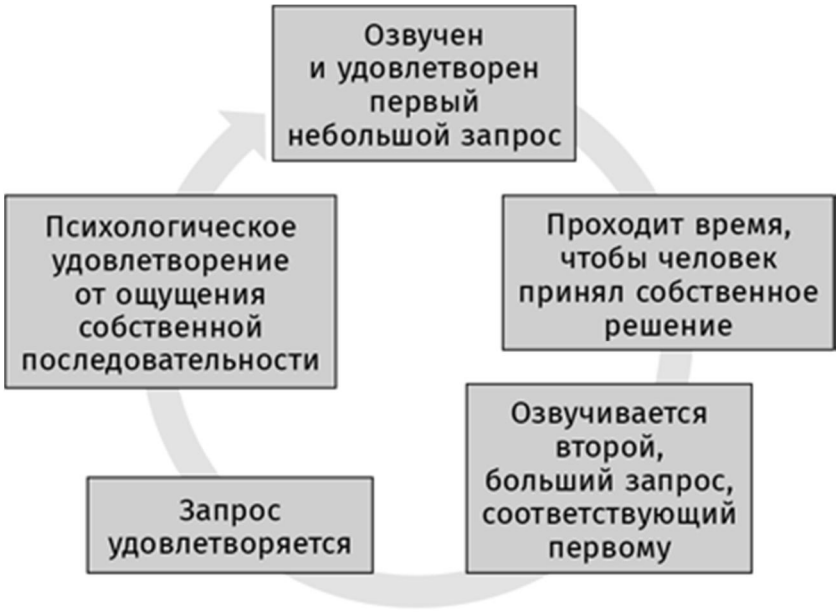
Нет и еще раз нет. Они изменили только размер знака. В ходе второго обхода домов владельцам сначала предлагали разместить на окне небольшую наклейку длиной меньше 10 см. А через несколько недель тех же людей просили установить большой и уродливый знак на видном месте — и 76% из них согласились.

Фридман и Фрейзер назвали этот подход «ногой в двери». Небольшая уступка со стороны объекта воздействия (размещение наклейки) на окне заставляла хозяев соглашаться и с последующей просьбой (установкой крупного знака).

С тех пор подобные эксперименты проводились неоднократно, и результаты каждый раз были просто поразительными. Выходило, что если человек сначала соглашается на небольшую уступку, то «показатели» последующего подчинения возрастают в разы.

Принцип последовательности в комбинации с правилами подчинения дают манипулятору огромную силу. На самом деле все мы хотим быть последовательными, просто чтобы казаться последовательным. Мозг не любит, когда мы сами с собой ведем внутренний спор. Поэтому иногда мы прыгаем выше головы только ради того, чтобы не сбиваться с ранее намеченного пути, даже если оказывается, что он был выбран неправильно. Если выбор уже сделан, мы стараемся сохранять последовательность. Наглядно этот механизм изображен на илл. 6.8.

ЗАМЕТКА Время, выделенное на то, чтобы обозначить последовательность и приверженность ранее выработанному мнению, не обязательно должно быть длительным — иногда достаточно и нескольких секунд. Если человек согласился на исполнение первого запроса, он, скорее всего, захочет быть последовательным, то есть согласится и со вторым.



Илл. 6.8. Последовательность в действии

Последовательность в работе социального инженера

Правило, которое я стараюсь всегда соблюдать: без экстренной необходимости не выходить из легенды. Причина, по которой можно отказаться от выбранной роли в процессе взаимодействия с объектом, должна быть действительно веской. Я поясню это, чтобы смысл описанных ниже событий стал вам понятнее.

Во время выполнения очередного задания мне предстояло работать в нескольких местах, и везде необходимо было пробраться к закрытым на

замок мусорным бакам. В них компания выбрасывала вышедшую из строя технику.

Чтобы пробраться к бакам, нужно было обойти охрану, проникнуть на закрытую территорию и потратить какое-то время на то, чтобы порыться в мусоре в поисках ценных находок.

Я применил сбор данных из открытых источников, чтобы узнать, какая фирма обслуживает эти мусорные баки. В компании, которая была целью атаки, придерживались строгой политики неразглашения информации о своих подрядчиках. Тем не менее я решил попробовать и позвонил в бухгалтерию, чтобы попытаться выведать эти данные в ходе беседы. Содержание нашего разговора с представительницей компании было примерно следующим.

Сотрудница компании: Добрый день, Бэт на связи. Чем я могу вам помочь?

Я: Бэт, меня зовут Пол, я из компании «Обслуживание мусорных баков». Мы недавно открыли филиал в этом регионе и теперь формируем клиентскую базу. Я хотел узнать, могу ли я куда-то отправить наше коммерческое предложение?

Сотрудница: Да, мы принимаем предложения от потенциальных подрядчиков. Просто пришлите нам информацию о перечне ваших услуг и их стоимости. Если нас заинтересует ваше предложение, мы с вами свяжемся.

Я: Отлично, спасибо. А подскажите, пожалуйста, ваш электронный адрес?

Сотрудница: Этими вопросами занимаюсь не я. Отправьте предложение на подрядчики@компания.com.

Я: Ага, понятно. А могу ли я как-то получить от вас обратную связь, что предложение дошло? А то мне уже несколько раз говорили, что писем моих не получали. Я совсем недавно устроился на эту должность и еще не до конца во всем разобрался.

Сотрудница: Ну что ж, ладно. Отправьте его на beth.p@компания.com.

Я: Бэт, вы просто моя спасительница. А можно задать вам еще один вопрос, немного необычный?

Сотрудница: Ммм, наверное.

Я: Я работаю в продажах уже давно, но мусорные баки — это для меня дивный новый мир. Так что я даже не знаю, насколько у нас конкурентоспособное предложение и цены. Не могли бы вы помочь мне сориентироваться в этом деле?

Сотрудница: О, сочувствую… Ну, знаете что, вышлите предложение, и я лично прослежу, чтобы его точно рассмотрели.

Я: Вы не представляете, как помогаете мне, Бэт! Знаю, что уже и так много попросил, но, может, вы подскажете, с кем мы конкурируем? [Видите: она уже решилась мне помочь, дала личный e-mail и вступила в беседу. Но достаточно ли сильный между нами раппорт для того, чтобы озвучивать такую просьбу?]

Сотрудница: Ох, Пол… [вздыхает и медлит с ответом]: Я бы с удовольствием, но в нашей компании на этот счет есть жесткие правила. Рада была бы помочь вам, но не хочу неприятностей на свою голову.

Я: Ничего страшного, Бэт, я понимаю. Прошу просто потому, что действительно не в курсе, как обстоят дела на рынке. Может быть, поступим так: я перечислю названия конкурентов, а вы кашлянете, когда услышите нужное? «Отходы на 5+», «Отличные мусорки», «Управление мусором» [Бэт покашливает.]... О, Бэт, я надеюсь, вы не простудились!

Сотрудница [усмехается]: Да уж, кажется, подхватила какой-то вирус. Что ж, удачи вам!

Эта информация помогла мне подобрать необходимую униформу, проникнуть на охраняемую территорию, найти жесткие диски и USB-флешки. Если бы сохранившаяся на них информация попала в плохие руки, это могло подставить под удар всю компанию.

Пользуясь желанием другого человека быть последовательным в своих действиях и мыслях, социальный инженер может добиться от него удовлетворения своих запросов.

Седьмой принцип: симпатия

Людям симпатичны те, кто похож на них самих. Людям симпатичны те, кому они сами нравятся. Эти принципы могут показаться странными, но их нужно понять и запомнить.

В пятой главе мы говорили о племенном мышлении. Сейчас я предлагаю вспомнить о нем в контексте утверждения: «Людям симпатичны те, кто похож на них самих». Если мы похожи, значит, мы из одного племени: нам друг с другом комфортно, мы знаем, как действовать. Мы нравимся, нас принимают, нам доверяют.

А теперь разберем второе утверждение: «Людям симпатичны те, кому они сами нравятся». Вспомните исследования Пола Зака, посвященные влиянию на нас окситоцина, — я рассказывал о них в первой главе. Согласитесь, они идеально сочетаются. Если человек нравится вам, он ощущает с вашей стороны симпатию и доверие. Как же ему после этого не начать симпатизировать вам?

И прежде, чем вы воскликнете: «Неужто все так легко?!», я перечислю несколько важных нюансов:

Симпатия должны быть искренней. Нельзя сымитировать симпатию и надеяться, что все сработает. Даже если объект воздействия поверит

вам вначале, неискренность обязательно раскроется. Скорее всего, это негативно повлияет на раппорт и доверие в будущем.

Комплименты не равны симпатии. Чтобы комплимент произвел желаемый эффект, он должен быть искренним и соответствовать уровню уже установленного раппорта.

Огромную роль играет невербалика. Если передаваемые вами невербальные сигналы тоже свидетельствуют об искренности (мы уже касались темы соответствия слов и языка тела в пятой главе), собеседнику будет проще вам довериться, почувствовать себя комфортно в вашем обществе и ощутить по отношению к вам симпатию.

Короче говоря, через все эти нюансы красной линией проходит идея о том, как важна искренняя, а не сыгранная симпатия. Мой друг Робин Дрейке добивается этого, представляя, что каждый его собеседник — герой реалити-шоу. Вам может не нравиться его образ жизни или поступки, но ведь они вам интересны и вы хотите узнать, что же будет дальше. Это и есть искренность, на основе которой можно выстраивать доверие и устанавливать раппорт. Так намного легче оказывать на человека влияние.

Чтобы усилить это чувство, вы можете сделать искренний комплимент, отзеркалить язык тела собеседника или использовать его лексику (только не превращайтесь в попугая!) — тогда в вашей компании ему будет комфортно. На илл 6.9 приведено схематичное изображение принципа влияния симпатии.

Симпатия в работе социального инженера

В ходе одной операции я собирался пробраться в здание, пристроившись на входе за кем-то из сотрудников. Я решил импровизировать, так что, когда я уже подходил к дверям, какого-то конкретного толкового плана у меня не было.

Илл. 6.9. Симпатия в действии

Тут я обратил внимание, как на парковке мужчина выходит из совершенно новой Kia и быстро направляется ко входу. Заняв удобную позицию, я достаточно громко, чтобы он услышал, спросил стоящую рядом женщину: «Не знаете, чья это Kia?» Женщина взглянула на меня, как на сумасшедшего, но это меня не особенно обеспокоило, потому что моя спонтанная задумка удалась: владелец машины обернулся:

— Это моя машина. Что-то не так?

Я протянул ему руку и сказал:

— Добрый день. Я — Пол из отдела управления персоналом. [Я понадеялся, что мужчина окажется из другого отдела, и мне повезло.] Извините, что побеспокоил. Я тут недавно работаю. Вот увидел вашу машину и хотел расспросить о ней, потому что мы с женой хотим такую же.

И я попал в точку. Мужчина с удовольствием бросился рассказывать об автомобиле, даже устроил мне небольшую презентацию прямо на парковке, так что через некоторое время я попросил его:

— Черт, уже опаздываю на встречу. Может, продолжим по дороге в офис?

— Никаких проблем, — ответил он, и мы двинулись ко входу в здание. Он продолжал рассказывать мне про гарантии от производителя, комфортабельность салона, расход топлива и т.п. Короче говоря, машина ему очень нравилась.

Когда мы оказались у поста охраны, я сказал:

— Складывается впечатление, что вы действительно выбрали лучший вариант. Где вы научились так хорошо разбираться в машинах?

Обратите внимание: здесь я не только похвалил его выбор, но и валидировал его знания. После этого он открыл дверь своим пропуском и придержал ее для меня, даже не задумавшись.

Чтобы не вызвать подозрения у охранника, я достал из кармана бумажник, приложил его к считывающему устройству и как ни в чем не бывало прошел за своим новым знакомым. Он еще 20 минут рассказывал про свою машину, пока мы, наконец, не оказались перед дверью в отдел по управлению персоналом, где и распрощались.

— Что ж, вам сюда, а мне в офис 4328. Если у вас возникнут вопросы, я с радостью отвечу, — сказал мужчина.

— Мне кажется, было бы проще попросить вас купить мне машину, так хорошо вы в них разбираетесь! Можно позвонить вам часа в три, когда закончится моя встреча?

— Да, пожалуйста. До связи!

И он скрылся за углом.

Мне нравилось то, что нравилось ему, а сам он понравился мне за его знания. Исключительно благодаря этому я прошел не только через пост охраны, но и спокойно передвигался по зданию, не привлекая к себе лишнего внимания.

Симпатия — мощный прием, способный открывать перед социальным инженером многие двери — в прямом и переносном смысле. Но, возможно, у вас возникнет та же проблема, что и у меня: мне было трудно научиться быть заинтересованным в человеке, чтобы симпатия выглядела подлинной.

СОВЕТ ПРОФИ Нельзя вести с объектом себя тепло и дружелюбно, а получив желаемое, сразу становиться холодным и равнодушным. Такие перепады не вызовут у объекта ничего, кроме негативных чувств.

Восьмой принцип: социальное доказательство

В 1969 году доктор наук Роберт О’Коннор провел исследование под названием «Модификация социальной изоляции через символическое моделирование» (Journal of Applied Behavior Analysis, 1969, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1311030/). В исследовании участвовали ученики младших классов, которые страдали повышенной тревожностью и переживали социальную изоляцию в школе.

Детей разделили на две группы. Первой показывали видео, в котором не происходило никакого социального взаимодействия. Второй группе продемонстрировали 23-минутный ролик, в котором дети активно общались и получали от этого удовольствие. После просмотра видео

поведение детей из первой группы никак не изменилось, а среди детей из второй группы наблюдались существенные улучшения. Более того, когда шесть недель спустя исследователь вернулся в школу для повторного наблюдения, дети из второй группы продолжали взаимодействовать с одноклассниками намного активнее.

Такая модификация потенциально устойчивой модели социальной изоляции произошла благодаря так называемому механизму социального доказательства. Фильм убедил детей из второй группы, что социальные взаимодействия для них безопасны и даже полезны.

Социальное доказательство в действии

В одном из выпусков прекрасного телешоу «Скрытая камера» (Candid Camera) проделали интересный эксперимент, который показывал, как сильно социальное доказательство влияет на самых разных людей. Три-четыре человека, якобы не знакомых друг с другом, заходили в лифт, а затем синхронно поворачивали назад. Пассажир, который не имел к ним отношения, автоматически следовал их примеру. Исключительно с помощью этого приема участниками розыгрыша удалось заставить одного молодого человека обернуться вокруг своей оси и снять шляпу!

Никто не хочет сильно отличаться от окружающих. Кто-то, возможно, возразит: я-то уникален и ни к какой группе не принадлежу. Возможно. Но и такие уникумы тоже представляют собой вполне определенную социальную группу.

Когда мы чувствуем себя потерянными, сбитыми с толку, когда мы не уверены, то обычно смотрим на других и ищем в их поведении подсказки, как нам стоит поступить, то есть ищем социальное доказательство.

Занимательная история

Однажды я показал вышеупомянутый выпуск «Скрытой камеры» на своей лекции в Вегасе. Пятеро моих студентов решили повторить этот эксперимент. Притворяясь незнакомцами, они сделали это трижды. И каждый раз люди, не знавшие, что в действительности происходит, следовали за группой.

Социальное доказательство в работе социального инженера

Мы часто не хотим совершать какое-либо действие первыми. Однако на практике я убедился, что использование социального доказательства существенно облегчает процесс принятия решения, которое сложно оценить однозначно.

Илл. 6.10. Социальное доказательство в действии

Как-то раз мне нужно было проникнуть в охраняемую часть одного здания. Для этого я, как смог, подобрал одежду, чтобы изобразить мастера по обслуживанию телефонов. Но, вместо того чтобы сразу идти в офис компании-объекта, сначала зашел в соседнее здание. Там я представился: сказал, что я — Пол из местной телефонной компании, которая обслуживает здание, и вручил своим новым знакомым фальшивую визитку.

Потом зашел к другим соседям компании-объекта и повторил те же действия. Наконец, я оказался в приемной целевой компании и произнес следующее:

— Меня зовут Пол. В последнее время поступают жалобы на сбои телефонной связи и интернета. Мне нужно проверить все компании в этом здании и выяснить, есть ли повреждения системных настроек.

Женщина, сидевшая за столом, пыталась меня перебить, но я ей не дал:

— Я только что поговорил с Бэт из соседнего офиса и проверил работу их системы — сбоев не обнаружил. И с Фредом, вашим соседом с другой стороны, встречался. Так что я решил: раз уж пришел, может, заодно протестирую и ваши системы. Надо убедиться, что сбоев в работе точно нет.

При этом я смотрел не на нее, а в свою записную книжку, якобы проверяя, какие офисы уже посетил. После этого у женщины не осталось сомнений в честности моих намерений:

— Наверное, Фред был счастлив, что вы пришли. Он все время жаловался на неполадки.

После этого она провела меня прямо в серверную.

Социальное доказательство я использовал во время интервью, фишинга, вишинга и др. Например, в ходе одного вишинга я озвучил свою должность и добавил: «Мне осталось сделать три звонка, и —

конец работе! Удачный сегодня день: большинство людей были со мной очень приветливы». Сразу после этого я перешел к запросу. В большинстве случаев применение легкого социального давления мне помогало, потому что собеседникам казалось, будто они не первые выдают мне информацию. Я считаю социальное доказательство одним из самых мощных средств влияния в моем арсенале.

Влияние или манипуляции?

Когда мы с учениками обсуждаем принципы влияния, они часто говорят: «То, что вы описываете, очень похоже на манипуляцию. Разве не этим вы занимаетесь?» Влияние и манипуляция действительно похожи, поэтому их часто путают.

Хочу сразу оговориться: я излагаю в этой книге свою точку зрения по теме, но ни в коем случае не считаю ее единственно верной. И когда к нам на подкаст пришел Роберт Чалдини, выяснилось, что его точка зрения кардинально отличается от моей.

Я считаю влияние «умением заставлять других хотеть делать то, чего хотите от них вы». А манипуляцией называю «умение заставлять других делать то, чего хотите от них вы». Разница в том, что манипуляция не предполагает заботы о чувствах объекта воздействия. Наконец, влияние обычно предполагает какое-то позитивное воздействие, а манипуляция — нет.

Манипуляция в действии

Проще всего проиллюстрировать отличия этих явлений с помощью истории, которой я, честно говоря, очень стыжусь и которая в то же время сильно повлияла на развитие моего бизнеса.

Решив стать профессиональным социальным инженером, я был уверен, что из игры всегда буду выходить победителем. Я считал, что любой не 100%-ный успех операции можно приравнивать к поражению. Из-за этого убеждения я не особенно задумывался о чувствах клиента, пока «побеждал».

Но однажды мне попался заказ, при выполнении которого я оказался безнадежно далек от успеха. Да что уж там, это был настоящий провал: мои объекты воздействия не реагировали на фишинговые письма и не кликали по моим ссылкам. Они сбрасывали мои вишинговые звонки. Заброшенные в офис флешки никто и не думал вставлять в компьютеры, как бы я их ни подписывал. Две попытки проникнуть на территорию с помощью классической схемы — с тяжелой коробкой — тоже не увенчались успехом.

Я был сбит с толку и расстроен настолько, что даже не похвалил эффективность системы безопасности клиента. Вместо этого решил

перейти на темную сторону. Я знал, что столовая, которой пользовались сотрудники компании, находилась за пределами здания, в которое мне не удалось попасть. Но в столовую-то вход был свободный.

Легенду выбрал следующую. Я — Фрэнк Т., руководитель нового проекта, запущенного отделом по управлению персоналом. Мне необходимо собрать информацию о том, насколько доступны сотрудникам услуги системы здравоохранения. А еще у меня есть секретарша Марша, измотанная жизнью мать-одиночка, — ее роль исполнила моя коллега. Придя в столовую, мы разыграли душераздирающую сцену. Марша подошла ко мне с опущенной головой и нерешительно отдала папку незаполненных бланков. Окинув их взглядом, я очень зло сказал: «Да что это за чушь! Ты же совершенно бесполезна…» Потом глубоко вздохнул и добавил: «Слушай, если ты не можешь справиться даже с такой банальной задачей, пожалуй, поищи другую работу, чтобы содержать себя и своего ребенка. А с МЕНЯ ХВАТИТ!»

Я раздраженно бросил стопку бумаг на стол и отошел в сторону. Марша опустилась на ближайший стул и заплакала.

Я заметил, как один мужчина направился прямиком ко мне, но, увидев слезы на лице Марши, повернулся к ней и спросил:

— У вас все в порядке?

Она подняла на него испуганные глаза и пролепетала:

— Да, конечно, простите. Я не хотела отвлекать вас от обеда. Но вы же знаете Фрэнка. Он так переживает.

— Фрэнк? Не знаю такого. Никто не имеет права так с вами разговаривать. Это просто неприемлемо! — возмутился мужчина и присел рядом с ней.

— Да нет, вы просто не понимаете. У него дома проблемы, а эти бланки нужно заполнить сегодня до вечера. А я просто о них забыла. Я думала, что заполню их за обедом, а он — видите: сорвался. Теперь он меня уволит.

— Но все равно его грубость непозволительна!

Но Марша перебила его:

— Да нет, это моя вина. Я должна была заполнить их еще на прошлой неделе. Теперь придется самой расхлебывать. Он на самом деле хороший человек и рисковал из-за меня.

— Сами вы виноваты или нет, ну-ка, дайте сюда ваши бланки!

Спаситель Марши пошел от стола к столу со словами: «Вообще-то заполнить эти бумаги нужно до конца дня, но постарайтесь сделать это до того, как приступите к обеду. А когда закончите — передайте вон той милой даме».

И он указывал на Маршу, которая улыбалась и благодарила его за доброту.

К моменту, когда был объявлен конец обеденного перерыва, у нас на руках были десятки бланков с личной информацией сотрудников: полные имена, даты рождения, сетевые ID, номера социального страхования, домашние и электронные адреса, номера телефонов и др.

Да, я «победил» — но какой ценой? Узнав, что ситуация была подстроена, какой вывод сделали сотрудники? В чем заключался урок для них? Не вести себя достойно, не сочувствовать ближнему? Согласитесь, это не очень-то поучительно.

Поскольку я прибегнул к манипуляции, то в этой компании за мной закрепилась репутация «чувака, который унижает секретаршу». Больше они меня к сотрудничеству не приглашали.

Принципы манипуляции

Манипуляция осуществляется по темным законам. Вот ее основные принципы:

- повышенная восприимчивость;
- контроль над средой;
- вынужденная переоценка;
- смещение власти;
- наказание;
- запугивание.

Даже по названиям этих принципов понятно, что речь идет о негативном явлении. Более того, есть одно исследование, которое только укрепляет меня в нежелании манипулировать.

В 1967 году исследователи из Пенсильванского университета Мартин Селигман и Стивен Майер изучили действия некоторых из вышеперечисленных принципов. Ученые проводили эксперименты на собаках: наблюдали за их реакцией на различные обстоятельства. Результаты они описывали в статье под названием «Приобретенная беспомощность» (Journal of Experimental Psychology, май 1967, http://homepages.gac.edu/~jwotton2/PSY225/seligman.pdf).

В ходе эксперимента собак сажали в клетки и подвергали ударам электрического тока. Одни животные находили выход: нажав рычаг на панели, можно было прекратить боль. Но другим такой возможности не давали, и эти собаки смирялись с невозможностью изменить ситуацию: они просто скулили от боли, лежа на полу, и даже не пытались сбежать. Они не сделали этого, и когда клетку открыли.

Об этом исследовании очень неприятно читать, но оно позволяет понять один из важнейших аспектов манипуляции. Часто объекты воздействия

принимают то, чего боятся, что приносит им боль, и совершают неправильные поступки просто потому, что не видят для себя другого варианта. Страх и злость мешают рассуждать рационально, и человек принимает эмоциональное решение. Так что когда профессиональный социальный инженер не дает человеку рассуждать логически, он лишает его возможности вынести из этого опыта что-то полезное. Узнав, что в ходе проверки кто-то манипулировал его страхами, объект воздействия откажется чему бы то ни было у вас учиться.

Что выбрать социальному инженеру: влияние или манипуляцию?

Профессиональный социальный инженер старается не просто выполнить задание, а чему-то научить при этом клиента. Следовательно, нужно отдавать предпочтение влиянию, а не манипуляциям.

Однако, прежде чем делать вывод о неуместности манипуляций в работе социального инженера, позвольте перечислить несколько ситуаций, в которых я все же использую манипуляции и не вижу в этом ничего плохого.

Мы довольно часто используем манипуляции в рамках деятельности фонда «Невинные жизни». Мы охотимся на «хищников», которые пытаются навредить детям и совершают ужасные преступления, а в борьбе с такими негодяями все средства хороши. Кроме того, я использую манипуляции, когда меня об этом просят сами клиенты. Обычно это происходит, когда ставки очень высоки: например, когда мой клиент — крупная финансовая компания, национальный гигант или организация, отвечающая за работу крупной инфраструктуры. В таких случаях проверки должны проводиться самым тщательным образом. Некоторые клиенты напрямую просят использовать манипуляцию, а не влияние, чтобы подвергнуть протоколы безопасности настоящему испытанию. Обычно такой запрос поступает после нескольких успешных проверок, когда клиент хочет перейти на новый уровень. Но даже при организации подобных тестов мы стараемся придумывать сценарии, которые в результате обучили бы клиентов чему-то полезному.

Например, одному клиенту необходимо было проверить работу лучших сотрудников телефонной поддержки. Вопрос стоял о защите информации стоимостью в миллионы долларов, и заказчику нужно было убедиться, что эти люди смогут противостоять самым жестким атакам.

Мы несколько раз попробовали применить к ним техники оказания влияния, но так и не выявили нарушений протокола безопасности. Тогда мы решили пойти еще дальше и придумали легенду, в которой приняли участие две представительницы моей СИ-команды.

Агент 1 позвонила в департамент и запросила информацию для заполнения платежной ведомости, используя при этом очень убедительную легенду.

СИ-агент 1: Добрый день! Меня зовут Сара, я звоню от компании АБВ. У нас только что уволили женщину, которая отвечала за заполнение платежных ведомостей, и сегодня эту задачу передали мне. А мне через неделю рожать, так что нужно закончить поскорее, прежде чем я уйду в декрет.

Представитель службы поддержки: О, поздравляю! Не переживайте, я вам помогу. Вам нужно только пройти верификацию, после чего мы перенастроим аккаунт, чтобы вы смогли в него войти.

СИ-агент 1: Отлично, спасибо. Ой!

Представитель службы поддержки: Сара, с вами все в порядке?

СИ-агент 1: Да, просто что-то странно кольнуло. Наверное, это просто стресс. Ничего, давайте все доделаем, и я, наконец, пойду домой. Что от меня требуется?

Представитель службы поддержки: Мне нужен номер аккаунта и PIN-код для идентификации.

СИ-агент 1: Сэр, но я же только что сказала: сотрудницу, отвечавшую за ведомости, уволили, так что PIN'а у меня нет. Она его поменяла, но теперь войти в аккаунт нужно мне.

Представитель службы поддержки: Простите Сара, но я не могу…

СИ-агент 1 [«начинает рожать» и бросает (но не выключает) трубку]: О господи, о господи, у меня воды отходят!

Представитель службы поддержки: Мэм, с вами все в порядке? Мэм?

СИ-агент 1 [кричит, будто бы обращаясь к коллеге]: Эй! Иди возьми трубку! [якобы обращаясь к другому коллеге]: А ты ВЫЗЫВАЙ СКОРУЮ!!!

СИ-агент 2: Алло, кто это?

Представитель службы поддержки: О боже. Это Стив из компании БВГ. Я помогал Саре войти в аккаунт с платежными ведомостями, но ей, кажется нужна помощь. Лучше побудьте с ней.

СИ-агент 1 [кричит неподалеку]: Если ты сейчас повесишь трубку, я тебя уволю. Нужно заполнить эти чертовы ведомости, или НИКТО НА СЛЕДУЮЩЕЙ НЕДЕЛЕ ЗАРПЛАТЫ НЕ ПОЛУЧИТ!

СИ-агент 2 [очень напряженно]: Ммм, Стив… Сара требует, чтобы я сначала решила проблему с доступом, в противном случае она отказывается ехать в больницу.

После этого Стив назвал номер аккаунта и всю необходимую нам информацию.

Изобретательно? Да. Манипуляция? Безусловно! Но компании было важно узнать, сумеют ли ее представители противостоять реальной атаке, организованной злоумышленниками, — это мы и проверили.

Конечно, список ситуаций, в которых вас могут попросить использовать манипуляции в процессе работы, на этом не исчерпывается. Тем не менее мы обговорили самые важные вопросы, которые вам необходимо обдумать, если вы собираетесь стать или уже являетесь социальным инженером. Будете ли вы использовать манипуляции? Если да, то в каких случаях? И в какой мере?

Принципы влияния и манипуляции действуют на большинство людей, не являющихся психопатами. Тем не менее чем чаще используешь «темные» методы, тем выше шансы перейти на темную сторону. Ведь невозможно выйти чистым из грязи. Исходя из этих соображений, я обязательно провожу беседы с командой участников фонда «Невинные жизни»: мы говорим о том, что манипуляции лишь тактика, допустимая в конкретных условиях. Для меня важно, чтобы работа не делала нас хуже. Поэтому в штате фонда есть психолог, который заботится о сохранении здоровой среды в коллективе, а также помогает сбросить груз любого негатива.

Резюме

Если бы вам можно было вынести из этой главы только одну полезную мысль, мне хотелось бы, чтобы она была такой. Вы — человек (равно как и я). Влияние работает — тут все просто и понятно. Оно действует и на объекты воздействия, и на вас. Этот процесс невозможно остановить, как ни пытайся.

Грамотное использование влияния даст вам то, что вы хотите. Люди будут вести себя и взаимодействовать с вами так, как вам надо. А если вы научитесь одновременно использовать влияние и навыки установления раппорта, то будете просто непобедимы.

Люди хотят рассказывать о себе. Люди хотят доверять.
Люди хотят подружиться с вами и помогать вам. Этот механизм настолько мощный, что, если не использовать его с осторожностью, он может буквально затмить ваш взгляд на мир — а там и до злоупотреблений недалеко.

Поэтому постоянно напоминайте себе, с какой целью вы пришли в социальную инженерию. Я, например, повторяю себе следующее:

- Я занимаюсь этим, чтобы помогать клиентам сохранять безопасность.
- Я делаю это, потому что у меня хорошо получается.
- Я делаю это, чтобы люди могли узнавать о возможных опасностях.
- Я делаю это, чтобы обеспечивать жизнь своей семье и своим сотрудникам.

Профессиональный социальный инженер обязан сохранять ответственное отношение к своей работе. Именно мера его

ответственности определяет, какие решения он будет принимать во благо клиентов, сотрудников и в собственных интересах.

Принципы влияния и манипуляции, которые мы обсудили в этой главе, ежедневно используются в маркетинге, рекламе, продажах, деятельности благотворительных организаций и т.п. Почему же не показать клиентам, какими опасными они могут стать в руках опытных мошенников и злоумышленников?

Не пожалейте времени, перечитайте эту главу несколько раз. Разбирайте каждый принцип по отдельности. Отрабатывайте его применение на коллегах и членах семьи — естественно, в пределах разумного. И постепенно он станет частью вашего коммуникационного арсенала, еще одной стрелой в колчане, которая поможет метко поражать ваши социально-инженерные цели.

Таких стрел у меня для вас заготовлено еще много. Например, в следующей главе мы обсудим навыки, которые я уже упоминал в предыдущих главах. Давайте же, наконец, поговорим о фрейминге и извлечении информации.

7 Оттачивая мастерство

> Искусство и наука объединяются в методе.
>
> Граф Эдвард Джордж Булвер-Литтон

Мне хотелось бы поговорить о социальной инженерии как об искусстве — этого аспекта я придерживался в первом издании моей книги. Такая точка зрения поможет прояснить особое значение данной главы. После того как вы смоделируете план коммуникации, продумаете легенду, освоите мастерство установления раппорта и использования техник влияния, вы должны будете применить все это на практике. Вот где наука фрейминга и извлечения информации встречаются с искусством!

Граф Эдвард Джордж Булвер-Литтон, британский политик и писатель XVIII века, писал, что именно в методе обнаруживаются точки пересечения искусства и науки. В этой главе мы обсудим, как профессиональному социальному инженеру научиться искусно извлекать информацию и с научной точностью проводить фрейминг.

Когда я только начинал работать поваром, мой начальник вручил мне мешок сельдерея и сказал: «Сделай мне соломку». Но я был новичком и понятия не имел, что ему надо. Несколько секунд спустя (хотя мне, конечно, показалась, что прошла целая вечность) он спросил: «Не понимаешь, чего я от тебя хочу?».

Я кивнул, а он вскрыл пакет, и буквально через минуту перед нами лежал сельдерей, нарезанный, как на илл. 7.1.

Илл. 7.1. Идеальная соломка из сельдерея

— Ага, нарезанный полосочками, — сказал я с выражением, словно был самым умным человеком на свете.

Я начал медленно и аккуратно нарезать оставшийся сельдерей, а шеф-повар наблюдал. Потом он сказал:

— Отлично справился. А теперь мне нужно, чтобы ты точно так же нарезал еще два пакета.

Я почувствовал уверенность в себе и попытался резать с такой же скоростью, как и он. Но, поскольку я забочусь о психологическом состоянии читателей, пожалуй, не стану помещать в эту книгу фотографию сельдерея с куском моего оттяпанного пальца.

Вы, вероятно, задаетесь вопросом, какое отношение эта история имеет к теме главы. Да самое прямое. Приготовление пищи — это искусство, в основе которого лежит наука по использованию инструментов (например, умение управляться с ножом). Шеф должен понимать, как сделать блюдо вкусным, — это его искусство. Но без науки приготовления еды (и защиты собственных пальцев) тоже далеко не уйдешь. А если искусство и наука сольются в единое целое — у вас появится шанс приготовить идеально сбалансированный кулинарный шедевр.

ЗАМЕТКА За годы работы на кухне я резал себе пальцы бесчисленное количество раз, так что теперь мои руки похожи на творение доктора Франкенштейна. И тем не менее части моего тела в составе блюда никогда никому не подавались. Просто подумал, что это стоит уточнить.

Эта глава должна показать вам, как слияние искусства с наукой фрейминга и извлечения информации способно вывести навыки, о которых говорится в первых шести главах книги, на уровень мастерства. Если научитесь правильно применять описанные в этой главе знания, то станете просто шефом мишленовского ресторана в мире социальной инженерии.

Динамические правила фрейминга

Вспомните конфигурацию своего дома или квартиры. Если смотреть снаружи, выдается ли какая-то из комнат вперед? У вас есть зимний сад необычной формы — или только прямоугольные жилые пространства? Где у вас расположены окна, как размещены двери и т.п.? Все эти детали можно назвать фреймами: они определяют ваше восприятие собственного жилища.

Фреймы (или, если угодно, точки зрения) в коммуникации действуют аналогичным образом. Я рассматриваю фрейминг — или то, как человек воспринимает и реагирует на определенную ситуацию, — как процесс, основанный на опыте и знаниях, полученных человеком в течение жизни. Фреймы меняются в зависимости от нового опыта.

Когда мне было 16 лет, мои мысли занимали серфинг и скейтбординг. Я думал, что жить стоит исключительно ради этого. И сейчас я приведу пример изменчивости фреймов как раз из того периода моей жизни.

Однажды мы всей компанией загрузили доски для серфинга в прицепы двух машин и посреди ночи поехали с западного побережья Флориды на восточное. Мы знали, что там ожидается сильный ветер и хотели поймать крутые волны.

Прибыли около пяти утра, через полтора часа должно было взойти солнце. Мы выгрузили доски и натерли их воском. До восхода, когда можно было бы нормально видеть, оставалось еще 30 минут, но нам не терпелось начать. Поэтому мы бросились в воду прямо в темноте, чтобы при первых лучах солнца уже рассекать волны. Мы слышали, как шумит океан и различали силуэты высоких волн вдалеке.

Мы вшестером вошли в воду и заплыли поглубже. Оставалось только ждать, покачиваясь на волнах. Каждые несколько минут мы слышали звук, напоминающий залп.

Поначалу он не особенно пугал нас, потому что доносился издалека. Но вдруг я почувствовал резкий запах, посмотрел на своих друзей и спросил: «Эй, а сейчас случайно не красный прилив?».

Красный прилив случается в определенное время года, когда массовое цветение водорослей убивает все вокруг себя и вода при этом приобретает очень специфический запах. Один из друзей ответил: «Да нет, еще рано. Не знаю, что это».

Прошло несколько минут, взошло солнце, и мы наконец увидели, что волны для серфинга просто идеальны. Кроме того, заметили группу рыбаков на пирсе неподалеку от нас: они кидали в воду приманку для акул. Когда те подплывали близко, рыбаки стреляли в них из дробовика: именно эти звуки мы и слышали. Короче говоря, оказалось, что мы с друзьями барахтались в воде, полной измельченной на приманку рыбешки. Ситуация была, безусловно, опасной, но мы только посмеялись.

Я глянул в воду и увидел под собой гигантскую тень. Я никогда не мог точно определить размер на расстоянии, но тут с уверенностью могу сказать: эта тень была гораздо больше моей доски.

Мы еще веселее рассмеялись, выгребли из рыбной каши на чистую воду и поймали несколько классных волн. Мне было 16, и серфинг был главной моей страстью, а опасность, которую представляли собой голодные акулы, ничего для меня не значила.

Вспоминая о том случае сейчас, почти 30 лет спустя, я понимаю, как сильно изменилась моя система ценностей. Сегодня мне даже думать страшно о той ситуации, хотя никакого океана, приманки для акул и серфинговых досок и близко нет. В 16 лет у меня не было никаких забот, тогда мне нравилась опасность. А теперь у меня двое детей, свой бизнес, я очень хочу жить. И мысль о том, что я барахтался когда-то в рыбной каше в окружении акул, не внушает мне ничего, кроме ужаса. Будь у меня машина времени, я бы сразу вернулся в прошлое, чтобы надрать самому себе задницу за такое безрассудство.

Мой жизненный опыт, возраст, осознание себя — все это сформировало определенный фрейм. Мысль, которую я сейчас озвучу, очень важна, так что вчитайтесь в нее внимательно. Фрейминг всегда динамичен, он далек от статики.

Фрейминг отражает одну особенность работы мозга: наше сознание реагирует скорее на контекст происходящего, а не на саму ситуацию. Вот несколько примеров:

- Луна, которую мы видим у горизонта, кажется больше, чем когда она находится прямо у нас над головой. Причина этого — в том, что мозг считывает контекст (место расположения объекта). А физический размер Луны меняться не может — это понятно.
- Мы никогда не говорим, что убиваем своих собак: мы их усыпляем. Такой фрейминг помогает справиться с болезненными переживаниями.
- В 1974 году Элизабет Лофтус продемонстрировала эффект фрейминга в своем исследовании, поменяв всего одно слово в предложении. Она показывала участникам эксперимента видео автомобильной аварии, а затем задавала один из двух вопросов:

  — Как быстро двигались машины до соприкосновения?

— Как быстро двигались машины до столкновения?

- В ответе на первый вопрос люди всегда называли меньшую скорость (подробнее об этом исследовании можно почитать по ссылке https://www.simplypsychology.org/loftus-palmer.html).
- В 1986 году Дэвид Сноу, Брук Рочфорд-мл., Стивен Уорден и Роберт Бенфорд провели исследование под названием «Процесс регулировки фреймов, микромобилизация и участие в движении» (Frame Alignment Process, Micromobilization, and Movement Participation) (https://www.jstor.org/stable/2095581?seq=1#page_scan_tab_contents), в которой выделили следующие аспекты фрейминга:
  - объединение фреймов;
  - усиление фреймов;
  - распространение влияния фреймов;
  - трансформация фреймов.

Сейчас я предлагаю обсудить объединение фреймов с позиции социального инженера. Скажем, вы оказались у входа в здание компании и увидели охранника. Его фрейм — не пропускать на территорию посторонних. Ваш фрейм — проникнуть в здание.

Если социальный инженер просто подойдет к охраннику и скажет: «Добрый день, мне нужно проникнуть в здание, кое-что украсть и оставить после себя хаос» — он вряд ли добьется своего. Не сработает даже, если, являясь профессиональным пентестером, вы скажете: «Знаете, я профессионал в области безопасности и мне нужно проверить, насколько эффективны ваши системы защиты. Так что пропустите меня, пожалуйста, а я взломаю ваш сервер».

Как же объединить ваши с охранником фреймы? Может, вы вспомните подходящий пример из уже описанных в этой книге? На илл. 7.2 изображена подсказка.

Легенда является тем самым объединяющим звеном: вы меняете фрейм объекта воздействия таким образом, чтобы человеку было проще принять ваши слова и действия. Подробное продумывание легенды (все эти детали, связанные с тем, как вы будете выглядеть, что возьмете в руки и т.п.) облегчает фрейминг. Но и это еще не все.

В 2004 году Джордж Лакофф написал книгу «Не думай о слоне!» (Don’t Think of an Elephant!, Chelsea Green Publishing), в которой описал самые важные для освоения искусства фрейминга правила. Я несколько адаптировал их к миру СИ.

Илл. 7.2. Легенда объединяет фреймы

Правило 1: все, что вы скажете, будет формировать фрейм

Чтобы по-настоящему разобраться в сути этого правила, представим процесс работы нашего разума — визуализируем входящую информацию. Великие учителя и рассказчики прославились благодаря своему умению рисовать словами яркие образы. Вот пример того, как по-разному можно описать одно и то же событие.

История 1. Сидя на доске для серфинга, я увидел, как на меня надвигается большая волна. Я лег на доску и стал грести, что было сил, но волна накрыла меня. Оказавшись под водой, я думал о том, действительно ли та акула была огромной, или мне только показалось.

История 2. Я посмотрел на горизонт, из-за которого едва выглядывало солнце. Лучи еще не освещали воду, но уже грели мне лицо. На меня, словно товарный поезд, надвигалась волна. По толщине и скорости движения волны было понятно, насколько она мощная. Белая пена на гребне была похожа на несущегося за добычей разъяренного льва.

Я лег на доску и развернулся к берегу. Я греб, максимально напрягая каждую мышцу тела. От напряжения казалось, что руки мои впиваются не в воду, а в жидкий цемент.

Волна подхватила меня, и началась бешеная гонка. Как ни пытался я устоять на доске, но в конце концов упал. И волна обрушилась на меня, словно разгневанный учитель.

Она несколько раз перевернула меня, и я оказался под водой. Оставалось только представлять себе голодных акул, учуявших мой запах. Я пытался не паниковать, забыть про страх: только бы выбраться на поверхность. Когда мне это удалось, я мертвой хваткой уцепился за доску и как умалишенный начал выгребать к берегу.

Обе истории описывают одно и то же событие. Но какая из них помогает полнее представить происходящее? Читая какой текст вам казалось, что вы находитесь в море вместе со мной?

Ответ очевиден: вторая история намного выразительнее. Теперь вы понимаете, почему это правило имеет такое значение? Иногда слова, которые мы используем в своем повседневном словаре, пробуждают в сознании объектов воздействия образы, которые кажутся им оскорбительными. Как профессиональный социальный инженер, я понимаю, что буду намного успешнее в своем деле и получу больше повторных заказов, если научусь избегать такого эффекта.

Не стану приводить полный список потенциально оскорбительных слов и выражений, лучше назову несколько обобщенных советов о том, от чего стоит отказаться.

- Расистские намеки. Даже сказанные в шутку, они неприемлемы в работе социального инженера. Шутить на такие темы бестактно, и это совершенно не смешно.
- Оскорбления, связанные с полом или сексуальной ориентацией. Подобные выпады производят такое же впечатление, что и расизм: выставляют вас невеждой и разрушают раппорт.
- Обсценная лексика. Даже если объект воздействия позволяет себе использовать грубые выражения, я старюсь обходиться без них. В первую очередь — чтобы защитить уши тех, кто будет слушать наш диалог, изучая отчет. В таких ситуациях собеседник часто подстраивается под меня и тоже перестает ругаться.
- Обсуждение функций тела. Эта тема может вызвать сильное отвращение, а потому ее стоит избегать.

Подумайте о словах и выражениях, из которых состоит ваш личный словарь. Подумайте, какие из семи базовых эмоций они способны вызвать у объекта воздействия: злость, удивление, страх, отвращение, презрение, печаль или радость. Если реакция на ваши слова и выражения может быть негативной и повредит ходу операции, не используйте их — хотя бы из предосторожности.

СОВЕТ ПРОФИ Мои коллеги занимаются так называемым «тестированием на проникновение». Что греха таить, само название подталкивает пошутить на околосексуальную тему. Тем не менее когда в очередной раз я слышу выражение: «Я поимел/изнасиловал их сервер», мне не до смеха. Только в США каждые 98 секунд кто-то становится жертвой изнасилования, так что я не вижу в таких шутках ничего смешного. На самом деле, если подобные шутки услышит человек, когда-либо подвергшийся сексуальному нападению, это может вернуть его в пережитую травму. Не используйте такие выражения для описания своей работы!

Правило 2: используемые в контексте фрейма слова оживляют его

Как-то вечером я вышел на крыльцо и увидел в углу у лампы паутину. Ее хозяин заворачивал какое-то насекомое в кокон, чтобы позже поужинать им.

Что я вам только что описал? Наверняка вы представили примерно то, что изображено на илл. 7.3.

К чему это я? Вы обратили внимание на то, что мне не пришлось употреблять слово «паук», чтобы сообщить вам о нем. Достаточно было описать его, и ваш мозг тут же представил его образ.

С помощью легенды социальный инженер заставляет объект воздействия думать о работе, которую якобы пришел выполнить. А описание ситуации также позволяет получить доступ к подходящему эмоциональному фрейму, не используя угрожающих слов напрямую.

Илл. 7.3. Если вы все еще не догадались, речь шла о пауке

Фото Artyangel, https://pixabay.com/en/spider-fly-web-insect-2683918/.

Однажды я отправил объекту воздействия фишинговый e-mail примерно такого содержания:

4 января камера наблюдения зарегистрировала проезд вашего автомобиля на красный сигнал светофора № XCV431. Назначенный за

это нарушение штраф до сих пор не был оплачен. Отказ от оплаты штрафа в означенный срок приведет к негативным последствиям.

Вы можете направить жалобу или подтвердить оплату штрафа на защищенном
портале www.пожалуйста_кликните_чтобы_я_вас_хакнул.com.

(Вы, наверняка догадались, что адрес страницы был изменен в целях безопасности.) Обратите внимание: я не угрожал объекту воздействия арестом. Страшные суммы штрафов называть тоже не пришлось. Просто с помощью слов я создал определенный образ, который вызвал у человека интерес и страх. А затем дал ему надежду на лучший исход. (Да, получатель перешел по ссылке.)

Правило 3: отрицание фрейма

Представьте себе такую ситуацию: один мой ученик получил задание — выведать у человека личную информацию (полное имя, дату рождения и пару фактов из жизни). И хотя ученик очень волновался, потому что я наблюдал за ходом беседы, разговор завязался быстро и буквально через минуту я услышал следующее:

Ученик: О, огромное спасибо за помощь. Я не знал, что подарить ей, а это отличная идея. [Ученик использовал приятную валидирующую формулировку в отношении идеи подарка жене, которую предложила собеседница.]

Объект: Никаких проблем. Знаете, мне… [Она собиралась сказать, что ей пора идти, но ученик не дал ей закончить.]

Ученик [протянул руку]: Меня зовут Том, Том Смит. [Он использовал приятное ритмическое построение фразы, чтобы подтолкнуть объект к раскрытию личной информации.]

Объект: Приятно познакомиться, Том. Я — Сара.

Ученик: Взаимно, Сара. А какая, говорите, у вас фамилия?

Объект: А вам-то зачем?

Ученик: Да так просто. Просто интересно. Слушайте, а что вы собираетесь устраивать на свой день рождения? Он же у вас в июле?

Объект: Ммм, Том, с вами было приятно пообщаться, но я не хотела бы об этом говорить. Извините.

Ученик: Никаких проблем, Сара. Я же не собираюсь использовать эту информацию для подбора паролей к вашим аккаунтам!

После этой фразы девушка буквально отпрянула от ученика, глянула на часы, сказала, что опаздывает, и быстро ушла.

Что он сделал не так? Мы называем это отрицанием фрейма — то есть высказыванием, в котором упоминается то, о чем объекту воздействия

думать нежелательно. Получается, вы сами подталкиваете его к невыгодным для себя размышлениям.

Как полагаете, к каким мыслям социальному инженеру не стоит подталкивать объектов воздействия в процессе общения? Наверное, на мысли о том, что их аккаунты могут взломать?!

Если не хотите пугать людей, не говорите страшных вещей вроде:

- «Да я не буду использовать эту информацию, чтобы вас взламывать!»
- «Ну я же не пытаюсь проникнуть туда, где мне быть не положено».
- «Я бы никогда не отправил вам зараженный e-mail».
- «Я не мошенник!»

Все это — примеры отрицания фрейма, возникающие, когда мы упоминаем нечто, противоположное фрейму. Но вспомните илл. 7.2: фрейм объекта воздействия — сохранение безопасности. Поэтому лучше не играйте с огнем.

Ищите способы подкрепления фрейма с помощью легенды, одежды и других инструментов: это поможет объекту воздействия избавиться от лишних вопросов и сомнений.

Правило 4: чем больше объект думает о фрейме, тем сильнее этот фрейм

Каждый раз, подталкивая человека задуматься о каком-либо фрейме, мы тем самым подкрепляем этот фрейм. Например, у родителей всегда есть выбор, какой фрейм укреплять — позитивный или негативный:

- «Ты такой глупый!»
- «Спорт — это не твое».
- «Можешь ты хоть что-то сделать правильно?»
- «Если захочешь, добьешься чего угодно».
- «Знаю, это сложно, но у тебя получится!»

Профессиональный социальный инженер может подкреплять фреймы не только словами, но и с помощью легенды.

Однажды, проводя вишинг, я выбрал легенду IT-специалиста из техподдержки: якобы он отвечает на жалобу о взломе пропускной системы, поступившей прошлым вечером. Нам нужно было получить полное имя, дату рождения, идентификационный номер сотрудника и некоторую другую информацию о человеке, ответившем на звонок. Диалог состоялся примерно следующий:

Объект: Добрый день, говорит Боб. Чем могу помочь?

СИ: Боб, это Пол из IT-отдела. Вчера вечером поступила жалоба на взлом пропускной системы, были отмечены 100 аккаунтов. Вам «повезло», вы в их числе. Скажите, возникли ли у вас сегодня проблемы при входе в здание?

Объект: Нет, все работало как обычно. Повторите, пожалуйста, кто спрашивает?

СИ: Пол, Пол Уильямс из IT. Я работаю с Тони Р. Это займет всего минуту. Вы наверняка знаете, что система пропусков связана с системой заполнения зарплатных ведомостей, так что решение этого вопроса лучше не откладывать.

Объект: Да уж. Так что мне нужно сделать?

СИ: Подтвердите ваше полное имя. Можете продиктовать вашу фамилию по буквам?

Объект: Мм, серьезно? Она же проще некуда: С-М-И-Т.

СИ: А вот и ошибка нашлась! В системе вместо Роберта Смита записан Роберт Джонс. Уж вы-то знаете, что бухгалтерия этому не обрадовалась бы. Наверное, когда злоумышленники запустили алгоритм, они изменил учетные данные в базе. [Я знал, что смысла в моих словах нет, но что-то мне подсказывало, что Боб из бухгалтерии не особенно разбирался в программировании.]

Объект: Действительно, не хотелось бы, чтобы мой чек получил кто-то другой. Давайте тогда проверим остальные данные?

Затем я выдал несколько заведомо ложных утверждений и положительное подкрепление сотрудничества. В результате объект назвал мне свое полное имя, дату рождения, идентификационный номер сотрудника и даже последние четыре цифры номера социального страхования. Мои слова и легенда подкрепляли фрейм, и объекту воздействия было проще его принять.

Пусть объект думает о вашем фрейме с самой первой фразы — тогда перейти к следующему шагу будет намного легче. К какому шагу? Конечно же, к извлечению информации.

Извлечение информации

Какое определение можно дать извлечение информации? Я определяю его, как «получение сведений, о которых вы не спрашивали». Извлечение информации со стороны выглядит, как обычный разговор. Но опытный извлекатель направляет беседу в нужное русло так, чтобы вы исподволь выкладывали необходимую ему информацию.

У тех, кто профессионально занимается добыванием сведений, есть свои наработки и правила, помогающие достичь успеха. Узнав о них и объединив воедино, как и подобает профессионалу от социальной

инженерии, вы в совершенстве овладеете искусством беседы. Эти навыки станут вашей силой, с которой принято считаться. А пока запомните одну важную вещь: правильный разговор, целью которого является извлечение вами нужной информации, непременно должен протекать, как непринужденная беседа.

В пятой главе я говорил о так называемом усмирении эго. Принцип, о котором я расскажу сейчас, является противоположностью такого усмирения, потому что вам нужно будет забыть о собственном эго и сосредоточиться на эго объекта воздействия.

Что такое эго? Оксфордский словарь английского языка дает следующее определение: «это ощущение индивидуумом самооценки и собственной важности». В данном определении необходимо разобраться. Автоматически многие полагают, что речь идет о своеобразном раздутии эго объекта — но это неверно. Потому что говорим мы только об обращении к эго.

А для этого нужно мысленно проставить три галочки:

- Вы должны быть искренними.
- Уже должен быть сформирован определенный уровень раппорта.
- Вы должны сохранять реалистичность.

Представьте, например, что к вам подойдет незнакомец и воскликнет: «О боже, никогда не встречал никого красивее вас!» Если после этого незнакомец попытается завести с вами разговор, то какие мысли пронесутся у вас в голове? Наверное, примерно такие:

- «Какой-то он странный!»
- «Что ему нужно от меня?»
- «Это какой-то развод?»
- «Согласен. А теперь проваливай!»

Формулировка не имеет значения — главное, что такое обращение к эго не будет искренним, реалистичным, поэтому и раппорта между вами и незнакомцем не будет никакого. Так что к успешному извлечению информации такой заход не приведет.

Сейчас расскажу вам одну историю. Ее главной героиней стала лучшая специалистка по извлечению информации, которую мне когда-либо доводилось встречать, — моя жена. Мы тогда приехали в Нью-Йорк и всей семьей решили поглядеть на мои пенаты. Добираться решили на метро. Если вы когда-нибудь бывали в нью-йоркском метро, то наверняка знаете, что там все держатся особняком. Никто не грубит, но и дружелюбия не проявляет. Все куда-то спешат, напряжены или устали. Так что никто ни к кому не лезет с разговорами.

Моя жена присела рядом с пожилой афроамериканкой, которая, как казалось, вот-вот уснет и пропустит свою остановку. Жена повернулась к этой женщине, потрогала краешек ее шарфа и сказала:

— Боже, какой он мягкий. Подскажите пожалуйста, где вы купили такой прекрасный шарфик?

Еще раз: мы ехали в нью-йоркском метро, и моя жена бесцеремонно нарушила личные, этнические, пространственные границы. И тем не менее она за считаные секунды подружилась с афроамериканкой! Почему? И где здесь обращение к эго?

Моя жена не только похвалила вкус женщины, но и попросила ее о совете. Причем сделала это совершенно искренне, что было сразу видно.

В результате между ними завязалась беседа на 20 минут, в процессе которой жена выведала все секреты о том, где в Нью-Йорке можно добыть отличную одежду. Я не очень этому обрадовался, потому что почувствовал приближение длительного шопинга. Но в то же время не мог не восхититься способностями моей жены: у нее можно было только поучиться.

Как же освоить мастерство извлечения информации на уровне Арисы? Какой секретный ингредиент использовать? Вот несколько подсказок:

- Она искренне любит людей и интересуется ими.
- Намерения у нее альтруистические.
- Она просто милашка и очень приятно улыбается.

Но что делать, если вы — не общительная, дружелюбная, миловидная и улыбчивая женщина азиатской внешности, как моя жена?

Для начала тренируйте наблюдательность. Например, на членах своей семьи. Вот вернетесь завтра домой с работы — и начинайте внимательно следить за происходящим вокруг. Помыла ли дочь посуду? Вынес ли сын мусор? Сделано ли их домашнее задание? А у жены как прошел день, так же напряженно, как у вас?

А затем попробуйте сказать что-то вроде: «О, кто-то помыл посуду. Большое спасибо!» или «Дорогая, вижу, ты сильно устала. Как прошел твой день?».

Оцените эффект, который произведут эти слова. Язык тела человека, к которому они будут обращены, смягчится. Ваши домашние откроются и, скорее всего, станут более разговорчивыми. Почему? Вы только что их похвалили (то есть провели валидацию) и обратились к их эго.

Вдоволь потренировавшись на семье, попробуйте применить этот навык с незнакомцами. Будет намного сложнее, потому что нужно четко провести грань между наблюдательностью и назойливостью, которая может испугать. Подходя к человеку, учитывайте все то, что мы

обсуждали в пятой главе. И, лишь убедившись в соблюдении всех необходимых условий, обращайтесь к его эго.

Представьте себе такую ситуацию: вы стоите в очереди в Starbucks позади объекта — высокого 34-летнего мужчины. Одет он очень аккуратно и стильно, но немного скучно. Вы замечаете, как он достает из кармана iPhone последней модели и начинает набирать сообщение. Как думаете, какое из этих наблюдений можно использовать для обращения к его эго? Что поможет завязать беседу? Сначала ответьте на этот вопрос сами, а потом уже читайте дальше.

Я бы попробовал что-то в духе: «Извините. Я обратил внимание на то, что у вас iPhone. Я все никак не могу решиться перейти на него. Скажите, вас все устраивает?»

Если человек только что выложил $1000 за смартфон, наверняка какое-то мнение по этому вопросу у него имеется. Вне зависимости от того, какое оно, выслушав его ответ, я бы сказал: «Ага, большое спасибо, вы мне очень помогли. Мне такие решения даются тяжело, но вы упростили задачу. Кстати, меня зовут Крис, Крис Хэднеги…» — и протянул бы ему руку.

Вот беседа и завязалась бы.

Общие интересы

Животрепещущие темы для обсуждения в современном мире найдутся всегда. Однако многие из них могут не просто разделять людей на сторонников и противников какой-то идеи, но даже порождать между ними острые конфликты. Когда такая тема всплывает в разговоре и выясняется, что собеседники придерживаются противоположных взглядов, некоторые начинают так страстно отстаивать свою точку зрения, что дело иногда доходит до неприкрытой агрессии.

Поэтому профессиональный социальный инженер должен не просто это понимать, но и уметь отстраняться от собственных мыслей на острые темы. В этом случае следует искать области, в которых имеются общие с объектом воздействия интересы.

Хочу привести пример из собственного опыта. Не буду говорить, каких взглядов придерживаюсь сам. Вы же представляйте все так, словно сами являетесь участником событий.

Я вошел в вестибюль бизнес-центра, в один из офисов которого я должен был проникнуть. У большого телевизора собралась группа людей. Оказалось, что случилось страшное событие — стрельба в школе. Погибли дети, было много раненых. Подросток, который принес в школу оружие и открыл огонь, совершил самоубийство. Настоящая трагедия.

Один мужчина сказал:

— Если бы я оказался там со своим пистолетом, этот придурок сдох бы еще до того, как успел в кого-то выстрелить.

Ему ответили:

— В этом-то и проблема! Если бы оружие было сложнее достать, подобные трагедии просто не происходили бы.

Присутствовавшие явно разделились на два лагеря. Чем больше людей выражали свое мнение по вопросу, тем напряженнее становилась атмосфера. Какая-то женщина встретилась со мной взглядом и, даже не поинтересовавшись, кто я, спросила:

— Слышали новости? Просто ужасно…

— Вот только сейчас узнал. Ужасная трагедия. У вас никто не живет в том районе?

— Слава богу, нет, — ответила она и тут же продолжила. — Но даже если бы и были. У Билла же есть решение: он бы вооружил всех до зубов, и мы бы снова жили, как на Диком Западе.

Билл, тот самый мужчина с пистолетом, тем временем все больше накручивал себя.

— Хорошо, тогда давайте лучше делать, как предлагает она: сидеть на попе ровно и молиться, пока они убивают наших детей, — воскликнул он, указывая на женщину.

Ауч! Ситуация накалялась очень быстро. Я понял, что сейчас не время для социальной инженерии, лучше сосредоточиться на том, чтобы разрядить обстановку. Когда Билл договорил, они с женщиной посмотрели на меня, как бы спрашивая: «Ну же, на чьей ты стороне?».

Стало понятно: чью бы сторону я ни принял, половина присутствующих на меня обозлится. Так что я воскликнул:

— Боже мой, как жаль их семьи! У меня у самого двое детей. Не представляю, как вообще можно пережить такую новость: что кого-то из них просто убили… Настоящая трагедия.

И вдруг пропасть, разделившая всех присутствовавших, исчезла. Люди смотрели друг на друга и видели, что речь не о том, кто за, а кто против свободного ношения оружия. Речь о наших детях. Любите вы оружие или ненавидите его — неважно. Все мы согласны с тем, что стрельба в школе — это ужасно.

Если в ходе выполнения своих профессиональных задач вам придется высказаться по теме, которая может обернуть многих людей против вас, постарайтесь найти и занять позицию, с которой все присутствующие согласятся. В большинстве ситуаций это сделать можно. А потом уже заводите нормальный, необходимый для решения социально-инженерных задач разговор.

«Опасная» тема не обязательно должна быть такой же серьезной, как в моем примере. Но лучше я перечислю несколько «легких» тем, которые помогают начать беседу с обозначения общих интересов.

Погода. Особенно ее аномальные проявления: сильный снегопад, ливень, нетипичный холод или жара. Погода — тема, способная растопить лед между незнакомцами.

Технологии. Попросите человека что-то посоветовать по поводу имеющегося у него гаджета (смартфона, ноутбука, смарт-часов и т.п.) — это отличная тема для беседы.

Дети. Здесь важно соблюдать два условия — и тогда вам удастся разговорить многих родителей. Во-первых, придерживайтесь правила о соответствии задаваемых вопросов существующему между вами и собеседником уровню раппорта. А во-вторых, задавайте общие вопросы, а не конкретно о детях объекта воздействия.

Домашние животные. Люди любят говорить о своих питомцах и показывать их фотографии.

Спорт. Справедливости ради надо заметить, что не все интересуются спортом. Но если вы заметите на человеке одежду или аксессуары со спортивной символикой, его любимая команда может стать отличной темой для обсуждения. Если, конечно, вы не скажете что-то вроде: «О, вы фанат “Ковбоев”? Сочувствую».

Я советую не затрагивать в разговорах политику, здравоохранение, религию и другие глубоко личные вопросы, а также информационные поводы, связанные с трагедиями. Эти темы способны развести вас с собеседником по противоположным сторонам ринга.

Наблюдая за окружением объекта (просматривая открытые источники и с помощью физического наблюдения), вы сможете найти тему, которая будет интересна вам обоим, а затем использовать ее, чтобы начать диалог.

Заведомо ложное высказывание

Это настолько мощное средство, что я настоятельно рекомендую вам как можно скорее его опробовать. Что вы сделаете, если в очереди в магазине услышите, как кто-то с уверенным видом выдает за факты явно ложную информацию?

Я наблюдал разные реакции: одни недовольно вздыхают или бурчат под нос «м-да» или «ну-ну», другие поправляют совравшего.

Почему мы так реагируем? Люди стремятся доказывать свою правоту, нам необходимо вносить коррективы в то, что, на наш взгляд, является неправильным. Когда мы слышим «абсолютно» неправильное высказывание, мы обычно его исправляем — хотя бы про себя. В зависимости от того, кем является человек, где он находится и насколько

для него важна тема, он и принимает решение: ограничиться внутренним диалогом или же озвучить свои поправки.

Приведу в качестве примера ситуацию, в свое время шокировавшую меня. Мы с Робином Дрейком сидели в ресторанчике. Накануне мы условились ради эксперимента озвучить в своем разговоре заведомо ложное высказывание и посмотреть, вызовет ли это реакцию у окружающих. Помещение было совсем небольшим, столы стояли недалеко друг от друга, так что при желании можно было без труда услышать, о чем говорят соседи.

Робин довольно громко спросил:

— Ты читал статью в Times, в которой говорилось, что около 80% людей используют свою дату рождения в качестве PIN-кода?

Исследований на этот счет на самом деле не проводилось, статья в газете никогда не публиковалась (и я всей душой надеюсь, что Робин ошибся в этой случайной оценке). Но я ответил:

— Неправда. Я, например, использую комбинацию цифр моей даты рождения и моей жены, то есть 0411.

Робин не согласился:

— А я вот думаю, это правда, потому что я как раз из тех, кто использует свои месяц и год рождения

Мы на пару секунд замолчали, и в разговор тут же включился сидевший позади нас мужчина:

— Я постоянно говорю жене придумать другой PIN-код, но она считает, что так проще его запомнить!

Жена не медлила с ответом:

— Конечно. 0660 — разве забудешь?

Ого! Женщина сообщила нам, двум совершенно незнакомым людям, свой PIN-код?! И ладно бы на этом дело кончилось — так нет же! Еще один мужчина, сидевший по другую сторону от нашего столика, обратился к женщине, с которой обедал:

— А у тебя какой PIN?

Та гордо ответила:

— В моем банке можно использовать шесть цифр, так что у меня в качестве PIN’а дата рождения дочери: 031192.

Все это услышала официантка и включилась в разговор:

— А мой банк разрешает использовать буквы, их просто нужно ввести с клавиатуры. Мой сын свою первую собаку назвал Самсоном, я это имя и использую.

И вот он я: сижу посреди ресторана и собираю даты рождения, имена домашних животных и, что самое пугающее, PIN-коды от банковских карт совершенно не знакомых мне людей — исключительно благодаря тому, что озвучил заведомо ложное утверждение!

Этот опыт произвел на меня неизгладимое впечатление, я стал использовать чудо-прием везде, где только возможно. И конечно же, я рассказывал о нем своим ученикам. Один из них, кстати, сам стал для меня в этой теме настоящим учителем. Когда я пересказал историю его группе на занятии, он воскликнул:

— А у меня появилась интересная идея! — и обещал раскрыть подробности позже.

Когда ему нужно было под моим наблюдением выполнить задание на взаимодействие с объектом, он подошел к женщине, которая сидела в кафе и ела клубнику. Молодой человек не делал никаких вступлений, даже не думал о раппорте — он построил разговор следующим образом.

Ученик: О, вижу, вы любите клубнику! Значит, вы наверняка родились в феврале.

Объект: Э… Нет, вообще-то в июле.

Ученик: Хм… Но тогда, наверное, 4-го, прямо в праздник?

Объект: Да нет, 11-го. А что? [Она удивленно на него посмотрела.]

Ученик: Ничего. До свидания.

Когда он вернулся ко мне, я сказал: «Но второй-то раз такое точно не сработает». Но он снова и снова подходил к незнакомцам, забрасывал их такими же странными ложными утверждениями — и каждый раз люди сообщали ему всю необходимую информацию!

У этого метода есть один серьезный недостаток — между социальным инженером и объектом воздействия не формируется раппорт. То есть по результатам взаимодействия собеседник остается в недоумении: что это было? И уж точно он не будет чувствовать себя лучше, чем до встречи с социальным инженером.

Поэтому при использовании заведомо ложных утверждений я рекомендую быть осторожными и помнить о следующих вещах:

- Если делать ложные утверждения слишком часто, вы рискуете показаться невеждой и потерять доверие объекта.
- Не путайте ложные утверждения и отрицание фрейма. Если не хотите, чтобы объект воздействия задумался о «взломах аккаунтов», не используйте это словосочетание в своих высказываниях.
- Заведомо ложные утверждения работают намного лучше, если применять их уже после установления раппорта с объектом.

- Заведомо ложное утверждение должно быть похожим на правду. Если бы мой ученик в своем эксперименте подошел к женщине со словами: «О, вы едите клубнику! Значит вы, наверное, летаете на драконах», — понятное дело, их общение ни к чему бы не привело. Он бы только сбил ее с толку, но не стимулировал ее стремление исправить неверную информацию.

Я серьезно призываю вас попробовать этот прием на практике. Вы удивитесь тому, насколько он эффективен и сколько информации позволяет получить.

В большинстве случаев, если вы подойдете к незнакомому человеку и попытаетесь узнать его PIN, дату рождения или другую личную информацию, это не вызовет по отношению к вам ничего, кроме подозрений. Однако если вы научитесь внедрять в разговор заведомо ложные утверждения, разглашение этой информации в беседе с вами будет казаться человеку намного более естественным.

Ложные высказывания и взаимный обмен

Вскоре я и сам опробовал метод своего ученика в ходе операции, целью которой был сбор аналогичной информации. Сработало как по мановению волшебной палочки. Только вот, получив информацию о дне и месяце рождения женщины, я сказал:

— Ага, 12 августа. Забавно, моя сестра тоже в августе родилась.

Я отплатил женщине такой же информацией, какую она дала мне, так что в результате у нее сложилось впечатление равноценного обмена. Потом я добавил:

— А бабушка нам всегда говорила, что августовские дети — самые артистичные и творческие. У вас, случайно, нет музыкальных талантов?

Женщина усмехнулась и ответила:

— Я скорее математик по складу ума. Поэтому и работаю бухгалтером. Видимо, даже бабушки иногда ошибаются.

— Пожалуй. Но лучше ей об этом не говорить. А то моя бабушка итальянка, она за такое может и подзатыльник отвесить, — ответил я.

— Прекрасно себе представляю. Моя семья ирландского происхождения. Вот уж где точно не стеснялись заниматься рукоприкладством! — подхватила собеседница.

— Ого! Звучит… интересно. Хм, так у вас, должно быть, и фамилия ирландская?

Мне показалось, что это — отличный предлог для сбора еще большего количества личной информации.

— Да уж более ирландское имя сложно придумать. Мари О’Доннелл, — сказала она, намеренно подчеркивая ирландский выговор.

— Какой у вас классный акцент! Эх, жаль я со своими итальянскими корнями совсем связь потерял, помню только ругательства.

— Тоже может пригодиться.

Обратите внимание: вслед за заведомо ложным высказыванием я применил метод равноценного обмена, благодаря чему узнал полное имя женщины, дату ее рождения, профессию и другие подробности из ее жизни.

Осведомленность

Не путайте осведомленность со всезнайством. Это совершенно разные вещи. Когда вы будете обсуждать с объектом воздействия разные вопросы, осведомленность откроет вам новые двери в процессе извлечения информации. Самое время рассказать историю еще одного моего провала, из-за которого сорвалась вся операция.

Мою компанию наняли для проверки безопасности системы доступа к серверу одного университета. В процессе предварительного изучения здания, в котором находилась серверная, мы обнаружили, что один профессор каждый день входил в него строго в 7 утра. Кроме него в такую рань в университете еще никого не было, так что это время показалось нам идеальным для попытки проникнуть в здание вслед за ним. На всех дверях стояли RFID-замки, но, поскольку мы специализируемся в первую очередь на социальной инженерии, то решили проникнуть к цели, используя влияние человеческого фактора.

Собрав из открытых источников данные о профессоре, мы узнали, что он написал статью по какой-то теме из квантовой физики, там было много незнакомых мне длинных слов. Благодаря своей безграничной мудрости и необузданному интеллекту (это сарказм, если что) я запомнил название статьи и запланировал личное знакомство с профессором на следующее утро.

И вот в 7:00 я увидел, как он быстро приближается к зданию. По моему сценарию, между нами должен был завязаться разговор о его статье, мы бы вместе прошли в здание, а потом каждый последовал своим путем (то есть я — прямиком серверную).

— Доброе утро, сэр. Меня зовут Пол Уильямс. А вы — профессор Смит, верно? — я пошел в наступление.

— Да, это я. Чем могу помочь? — ответил он, даже не замедлив шага.

— Я хотел задать вам несколько вопросов о вашей статье по квантовой физике, — сказал я, а затем на одном дыхании выпалил название публикации.

После небольшой паузы он сказал:

— Ладно. Что именно вас интересует?

О нет! Как я вообще мог не подумать о том, что он задаст такой вопрос? Мы продолжали идти рядом, но казалось, что между нами разверзлась бездна. Я честно пытался придумать хоть что-то умное, но не нашел ничего лучше, чем неуверенно спросить:

— Почему вы решили написать эту статью?

Впервые с начала нашей встречи профессор остановился, повернулся ко мне и сказал:

— Не знаю, что вы задумали, сынок, но лучше нам поговорить после того, как вы ее все же прочитаете.

И, не дожидаясь ответа, он еще быстрее зашагал к двери.

Безусловно, я мог бы прочитать его статью. Но сделай я это хоть 20 раз — едва ли придумал бы хотя бы пару толковых вопросов по существу. Я мог бы найти человека, разбирающегося в теме, чтобы тот помог сформулировать эти вопросы. Тем не менее к цели эти действия меня едва ли приблизили бы. Проще всего было изначально использовать легенду, соответствующую реально имеющимся у меня знаниям. Я мог бы притвориться студентом в поисках аудитории, где этот профессор будет читать лекцию. Мог бы обратиться к нему с вопросом, какую литературу почитать, чтобы вынести из его курса максимальную пользу.

Обращаясь к нему, мне нужно было уже обладать информацией об университете: курсах, преподавателях, программах. Осведомленность в подобных вопросах не подразумевает необходимости тут же вываливать все имеющиеся знания собеседнику, но они нужны, чтобы говорить убедительно. То есть если бы он спросил, какие курсы я уже посещаю, я смог бы дать ему правдоподобный ответ.

А чем правдоподобнее ваши слова, тем проще объекту воздействия поверить в то, что вы действительно являетесь тем, кем назвались.

Вопросы

Вопросы — естественная составляющая общения. Едва освоив умение разговаривать, человек быстро переходит к использованию вопросов для отправки и получения новой информации. Поэтому очень важно понимать, какие типы вопросов существуют (их всего четыре), а также уметь грамотно применять их в процессе извлечения информации. Это ключевой момент для профессионального развития социального инженера, и именно о нем мы сейчас поговорим.

Вопросы — прекрасный инструмент. Стоит нам услышать вопрос, как наш мозг тут же генерирует реакцию. И даже если мы не собираемся проговаривать ответ вслух, его мысленной формулировки все равно не избежать.

Умелое использование разных типов вопросов помогает вовлечь собеседника в разговор. Опытный социальный инженер подбирает тот

тип вопроса, который больше всего подходит для извлечения информации или получения от собеседника необходимой эмоциональной реакции.

И чтобы проиллюстрировать специфику использования разных типов вопросов в СИ, расскажу вам еще одну историю из личного опыта. Я называю ее «Операция “Офисное пространство”».

Мне нужно было получить доступ на 16-й этаж офисного центра. Компания, помещения которой расположились на этом этаже, арендовала их у владельца здания. Я придумал легенду инспектора из головного офиса компании, который без предупреждения явился для проверки соблюдения требований техники безопасности (например, не заблокированы ли эвакуационные выходы).

Легенду я выбрал на основе открытых источников: недавно в прессу просочилась информация о том, что сотрудники жалуются на плохие условия работы. Руководство компании пообещало эти проблемы разрешить: были приняты новые правила, и менеджеры местных офисов получили надлежащие распоряжения.

Я сделал бейдж с логотипом компании, на котором жирным шрифтом надписал: «Инспектор по безопасности». Вооружившись планшетом, камерой и парочкой дополнительных инструментов, я уверенно зашел в вестибюль и направился к лифтам, минуя пост охраны.

Женщина, сидевшая за столом, тут же вскочила и окликнула меня:

— Извините, сэр, куда вы направляетесь?

Я на ходу ответил:

— На 16-й.

— Пожалуйста, остановитесь. Мене нужно вас зарегистрировать, иначе вы не сможете подняться: у вас нет пропуска для лифта.

— О, прошу меня извинить. Сейчас я все объясню. Как к вам обращаться, мадам?

— Алисия Смит, — указала женщина на свой бейдж.

— Приятно познакомиться, Алисия. Я работаю на компанию АБВ, офис которой находится на 16-м этаже. В связи с неприятными событиями, недавно произошедшими в одном из наших региональных отделений, меня назначили ответственным за проведение внеплановых проверок во всех наших подразделениях. Руководителей на местах, по понятным причинам, не предупреждали. Вы, наверное, слышали, что люди жаловались на условия в наших офисах?

Она пожала плечами и сказала:

— Слышала в новостях.

— То есть вы в курсе, какие у нас проблемы. Уверен, что ваш работодатель заботится о вас. Руководство компании организует такие

инспекции, чтобы удостовериться в соблюдении нормальных условий труда сотрудников. Как вы понимаете, если не делать такие проверки неожиданными, они не будут эффективными.

— Да, это понятно. Хорошо, что ваша компания серьезно отнеслась к ситуации. Сейчас я пропущу вас в лифт.

И мы вместе направились к служебным лифтам. Но вдруг я остановился:

— Алисия, но ведь чтобы спуститься, мне тоже понадобится пропуск. Или какая у вас система безопасности в лифтах?

— Действительно, какая же я глупая. У нас недавно установили новую систему, так что пропуск действительно понадобится. Сейчас выдам вам карточку посетителя. Подождите меня минуту.

Она сбегала к своему посту, выдала мне пропуск, не потребовав каких-либо подписей, и мы попрощались.

Когда я вышел на 16-м этаже, то оказался в коридорчике, по обеим сторонам которого были стеклянные двери. Справа через такую дверь я увидел стол секретарши: она с большим интересом разглядывала меня. Я направился к ней и, понимая, что сейчас женщина обязательно начнет задавать вопросы, решил ее опередить:

— Добрый день. Меня зовут Пол, я из головного офиса компании, — я показал ей бейдж, но быстро его спрятал, так как не был уверен, что он похож на реально используемые в компании. Затем достал ручку и, сделав вид, что сейчас буду что-то записывать, спросил: — Это офис 43211, верно?

— Все верно, Пол. А с какой целью вы пришли? Не вижу вашего имени в списке посетителей, — сказала секретарша смущенно.

— А меня там и не должно быть. Я провожу внеплановую проверку. В прошлом месяце в компании возникали проблемы с соблюдением техники безопасности и норм гигиены труда. Так вот, руководство запустило специальные инспекции, чтобы проверить, были ли улучшены условия труда сотрудников. Вы же получали соответствующее уведомление?

Она кивнула и сказала:

— Да. Я должна была его распечатать и раздать копию каждому сотруднику.

— Отлично. Значит, я могу поставить первый плюсик, — сказал я, перелистнул страницу и отметил одну из граф в таблице. — Очень радует, когда проверка начинается с чего-то хорошего. Мне хотелось бы упомянуть ваше имя в списке сотрудников, выполнивших новые требования. Как вас зовут?

— Бэт. Бэт Симмонс.

— Отлично, Бэт. Вы, как мне кажется, девушка наблюдательная. Может, сразу и подскажете, к чему здесь нужно присмотреться внимательнее? С чего стоит начать?

Она быстро отвела глаза, но потом сказала:

— Мне кажется, у нас все соблюдается как нужно. Но я не уверена. Не хотела бы кому-то создать неприятности.

— Понимаю, Бэт, ничего страшного. Спасибо за честность. Тогда начну проверку. Я еще вернусь к вам, когда закончу.

И я свободно пошел бродить по офису.

Открытые вопросы

Открытые вопросы, как и следует из их названия, не предполагают какой-то конкретной формулировки ответа. Скорее они позволяют собеседнику ориентироваться на собственное мнение. На открытые вопросы обычно нельзя ответить просто «да» или «нет», и, значит, человек сам решает, какой объем информации раскрыть. Он ощущает одновременно свою власть в процессе разговора и валидацию с вашей стороны, что способствует установлению раппорта. Открытым можно считать, например, такой вопрос: «Какой ресторан в городе нравится вам больше всего?». А вот «Есть ли хороший ресторан рядом с этим отелем?» — вопрос закрытый. Оба вопроса могут быть уместны в конкретной ситуации, но первый дает возможность лучше изучить собеседника. Открытые вопросы вызывают определенные эмоции, и они звучат в ответе. Объект воздействия получит возможность продемонстрировать свои знания, отношения, убеждения, точку зрения, чувства.

Успех вашего взаимодействия во многом зависит от того, как вы, социальный инженер, будете использовать навыки активного слушания и куда станете направлять вопросы для получения полезной информации. Это важно понимать, чтобы уже на стадии легендирования определить типы вопросов, использование которых естественным образом впишется в общение. Помните, ваша цель — помочь объекту воздействия открыто заговорить про важные подробности, которые помогут вам достичь поставленной заказчиком цели с помощью социальной инженерии.

СОВЕТ ПРОФИ Девиз «Пусть просто продолжают говорить» для социального инженера не очень подходит. Ведь наша задача состоит не в том, чтобы разговорить собеседника, а в том, чтобы получить от него нужную информацию.

В ходе «Операции “Офисное пространство”» я неоднократно использовал открытые вопросы. Вспомните, например, мой вопрос про лифты. Алисия не только ответила на него, но и продолжила рассуждать о нововведениях в политике безопасности. Таким образом, использование открытых вопросов позволило мне не только получить

заветный пропуск, но и собрать важнейшую информацию об охране здания.

Закрытые вопросы

Закрытые вопросы позволяют получить короткие и конкретные ответы, состоящие всего из нескольких слов. Опытные специалисты часто используют такие вопросы для подтверждения собранной ранее информации. Кроме того, закрытые формулировки идеально подходят для оценки невербальных сигналов собеседника. Ведь наше тело автоматически отвечает на закрытый вопрос еще до того, как мы успеваем произнести ответ. Причем обычно невербалика не врет, даже когда вслух мы говорим неправду: например, мы пожимаем плечами или отрицательно качаем головой, а на словах соглашаемся.

Я часто использую закрытые вопросы в общении с детьми. Например, я могу сказать: «Я просил тебя лечь спать в 11. Действительно ли ты выключил компьютер в 11 и лег в постель?». Если, отвечая: «Наверное, да. Я не смотрел на время», сын мотает головой, становится понятно, что произошло на самом деле.

Закрытые вопросы также помогают уточнять или подтверждать конкретные факты. Причем, прежде чем переходить к конкретике, имеет смысл сначала задавать более общие вопросы. В частности, для начала беседы подходят вопросы, начинающиеся со слов «кто», «что», «где», «почему» и «как».

В «Операции “Офисное пространство”» я использовал закрытый вопрос, когда спросил секретаршу Бэт, получила ли она уведомление об изменениях в политике безопасности. Она не только кивнула, но и подтвердила свое согласие словами. Однако, когда я задал аналогичный вопрос о том, есть ли, на ее взгляд, проблемы с соблюдением этой политики в их офисе, Бэт согласилась, но при этом пожала плечами. Несоответствие между словами и действиями указало мне на то, что в своем последнем ответе она не уверена. Увидев ее замешательство, я мысленно отметил для себя несколько важных моментов.

Наводящие вопросы

Мне отправили ссылку на страницу, где было размещено видео с подписью: «Только самые наблюдательные и умные зрители смогут точно сосчитать, сколько раз люди в белых футболках перекидывают мяч».

Я подумал: «Я же социальный инженер, а мы самые наблюдательные представители рода человеческого. Проще простого!» И кликнул на ссылку.

Я специально пялился в экран, не отворачиваясь и не моргая, — усердно считал каждую передачу мяча. Когда видео закончилось, мне

предложили несколько вариантов ответа. Увидев правильный, я победно вскрикнул: «Ага!!!»

А затем закадровый голос произнес:

— Но кто из вас обратил внимание на мужчину в костюме гориллы, который пританцовывая прошелся через весь зал и вышел из кадра?

Я не поверил своим ушам: «Не было там никакой гориллы!» В конце концов, я социальный инженер, самый наблюдательный представитель рода человеческого. Не мог же я упустить что-то настолько очевидное!

Я снова запустил видео и, к своему изумлению, увидел высоченного мужчину в костюме гориллы, который пританцовывая прошелся с одной стороны кадра в другую, обернулся вокруг своей оси и исчез из зоны видимости.

Как я мог его не заметить?

На самом деле все предельно просто. Наводящий текст заставил меня сосредоточиться на строго определенном аспекте: я внимательно считал, сколько раз люди в белых футболках перекинут друг другу мяч. Все остальное мой мозг попросту игнорировал.

Так как же социальному инженеру использовать наводящие вопросы? В одной из описанных выше операций мне удалось заставить объект воздействия задуматься о том, что случится, если я не попаду в офис гендиректора. Я добился этого за счет комбинирования утверждения и наводящего вопроса: «Я прекрасно понимаю: меня не ждали, но как вы объясните начальнику, что мне не удалось решить проблему с его компьютером, когда он вернется из отпуска?»

Кроме того, я часто использую наводящие вопросы и ложную информацию еще на этапе проникновения в здание. У меня есть планшет со встроенной камерой. Отверстие у нее большое, размером с четвертак, да еще и с выступающей линзой, а рядом — отверстие поменьше для микрофона. Я постоянно беспокоюсь, что объект воздействия их заметит. Поэтому я закрепляю на планшете разные «деловые» бумаги и, обращаясь к объекту, постукиваю ручкой по какому-нибудь бланку со словами типа: «Видите? Я должен посмотреть серийный номер двигателя и проверить, не нужно ли его отозвать». Практика показывает, что камеру не замечает никто, потому что я направляю внимание собеседника в другую сторону.

Социальный инженер должен продумывать использование наводящих вопросов заранее. Встраивать их в легенду. Планировать действия, которые отвлекут объект от ненужных вам подробностей.

Например, в ходе «Операции “Офисное пространство”» я не хотел, чтобы Бэт внимательно рассматривала мой бейдж. Если бы с ним что-то оказалось не так, она бы это заметила, поэтому я быстро перевел ее внимание на бумаги, которые держал в руках. Это позволило мне не

только управлять вниманием собеседницы, но и создало иллюзию легитимности моего запроса.

Вопросы-допущения

В процессе извлечения информации социальный инженер может использовать допущения в форме утверждений и вопросов. Применять такие вопросы стоит в случае, если определенные знания у вас есть, но нужно проверить их истинность.

Эту технику я использую также, когда хочу выяснить, говорят ли мне дети правду. Например:

Я: И когда ты был на вечеринке, Тэмми тоже пришла?

Мой ребенок: Сильно позже меня. Так что не переживай, пап.

Несколько фраз — и я уже знаю, что сын действительно был на вечеринке. Так что, если мне нужно будет получить еще какую-то информацию, можно исходить из этого.

Профессиональный социальный инженер может использовать вопросы-допущения на стадии знакомства с объектом. Этот прием позволяет обойти нежелательные темы и не дать объекту воздействия резко прекратить обсуждение определенного человека или предмета.

В ходе «Операции “Офисное пространство”» я использовал допущения при знакомстве и с Алисией, и с Бэт. Допущение заключалось в том, что я находился на своем месте и они должны были понимать, почему обязаны пустить меня на закрытую территорию. Я не вел себя надменно и не злился — вместо этого сформировал у них ощущение того, что нахожусь там, где должен: ведь я сам точно знаю, с какой целью пришел и что обязан сделать.

Резюме

Своей многослойностью беседа похожа на лук. Один за другим вы снимаете слои, приближаясь к сердцевине, к сути.

Каждая техника извлечения информации важна для эффективного выстраивания диалога. Научитесь применять их — и станете мастером общения и социальной инженерии. Ваша цель — превращать извлечение любой информации в обычную, не вызывающую подозрений беседу. А для этого нужно снова и снова оттачивать описанные выше навыки. И что самое интересное, эффект не ограничится только вербальной коммуникацией: те же самые приемы отлично работают при ведении деловой переписки, в чатах, по телефону и т.д.

Как шеф-повар, решающий, какие инструменты и ингредиенты следует использовать для приготовления конкретного блюда, вы сможете добавить в общение несколько вовремя заданных вопросов, щепотку

заведомо ложных утверждений и замесить все это в достаточном количестве взаимного интереса, чтобы в результате получить необходимую информацию.

Со временем извлечение информации в ходе беседы станет получаться у вас так же ловко, как у шеф-повара приготовление фирменного блюда. Это предпоследняя стрела в вашем колчане. Еще про одну, без которой не обойтись ни на одном задании, я расскажу в следующей главе. Переходим к обсуждению невербальных сигналов и языка тела.

8 Я знаю, о чем ты молчишь

> Мы несем ответственность за развитие своего эмоционального интеллекта. Этот непростой навык не заложен в нас природой, поэтому мы сами должны его освоить.
>
> Пол Экман

Когда я готовил первое издание этой книги, мир невербальной коммуникации был для меня чем-то новым. Но уже тогда мы познакомились с доктором Полом Экманом, и он стал моим учителем. Его путешествие по миру невербалики началось в конце 1950-х, и последующие 60 лет он оставался ведущим исследователем в этой области.

Пол Экман помог мне не только улучшить эту книгу, но и существенно прокачать навыки общения. Благодаря нашему сотрудничеству, вышла моя вторая книга, «Разоблачение социальных инженеров: Человек в системе безопасности», в которой подробно разбираются мимика, язык тела, жесты рук и все остальные аспекты невербального общения. Я даже рассказал о том из них, какой невооруженным взглядом не заметишь: раскрыл тайны приручения миндалевидного тела.

Если вам доводилось читать мои тексты или слушать выпуски передач, в которых речь идет о докторе Экмане, вы, наверное, не удивитесь, что я реагирую на него как фанаты на музыканта на илл. 8.1.

Работая над этой главой, я ставил перед собой несколько целей. Во-первых, старался соответствовать высоким стандартам Пола Экмана и использовать только подтвержденные исследованиями данные. Во-вторых, я не хотел дублировать свои ранние книги — это было бы неприятно тем, кто уже прочел одну из них или обе. Поэтому в этой книге мне хотелось бы обсудить невербальную коммуникацию в крайне важном для социального инженера аспекте — понимании того, что отличает комфортное состояние от дискомфортного.

Источник фото: https://commons.wikimedia.org/wiki/File:Elvis_Presley_-_TV_Radio_Mirror,_March_1957_01.jpg.

Илл. 8.1. Многие полагают, что, приближаясь к Полу Экману, я веду себя так (и это недалеко от истины)

В этой главе я в пух и прах разнесу неверные представления о языке тела и покажу, на что действительно стоит обращать внимание профессиональным социальным инженерам.

Роль невербалики

Прежде чем перейти к основной части этой главы, я хочу объяснить вам, почему так важно учиться считывать невербальные сигналы. И конечно, лучше всего сделать это с помощью истории.

Когда мы с Полом Экманом работали над книгой «Разоблачение социальных инженеров», он проверял, насколько точно и логично я излагаю информацию и есть ли у нее научные подтверждения.

Одну из глав я посвятил исследованию зеркальных нейронов. Предполагается, что в мозге существует группа нейронов, ответственная за отзеркаливание невербальных сигналов, поступающих к нам от других людей.

Исследования самого Экмана показывают, что, когда мы ощущаем какую-то эмоцию, она проявляется у нас в непроизвольной реакции — микровыражениях[16]. Кроме того, известно, что, когда мы воспроизводим то или иное выражение лица, мы пробуждаем в себе связанную с ним эмоцию.

На основании этого я заключил: раз зеркальные нейроны позволяют «отзеркаливать» выражения лиц других людей (вслед за которыми возникают и соответствующие эмоции), получается, что мы можем контролировать эмоциональные переживания объектов воздействия.

Пока я работал над «Разоблачением социальных инженеров», в научном мире развернулись активные дебаты на тему зеркальных нейронов и связанных с ними исследований. Поэтому Пол Экман написал мне приветливое электронное письмо, в котором спрашивал: «Хотите ли вы, чтобы ваша книга пестрела отсылками к устаревшим или оспоренным исследованиям? Ведь многие из нынешних гипотез могут не подтвердиться».

Мой ответ был примерно таким: «Но как же… у меня уже страниц 40 написано об этом! И главу нужно сдать через пять дней…» Я будто просил у доктора Экмана разрешения: «Ну ладно, тогда пишите».

Но он ответил иначе: «Что же, значит, у вас есть пять дней на то, чтобы прочитать вот это исследование о миндалевидном теле и переписать главу на основании новой информации». В результате я написал целых 60 страниц про отдел мозга, о котором только что узнал.

Безусловно, Экман очень мне помог, и из этой ситуации я вынес для себя три важных урока:

- Необходимо разбираться в том, как работают используемые мной методы, если я действительно хочу помогать своим клиентам.
- Важно использовать и адаптировать новые исследования.
- Сон — штука крайне недооцененная.

Так вот, пока я писал главу об укрощении миндалевидного тела, я снова заметил связь между исследованиями о пробуждении эмоций у объекта воздействия и контроле их реакций. Раз миндалина способна создавать эмоциональные стимулы еще до того, как сознание успеет «включиться» в процесс, значит, я смогу воспользоваться эмпатической реакцией объекта в своих интересах, при условии что мне удастся вызвать у него ощущение легкой грусти или страха.

Иными словами, освоение искусства использования легенд поможет мне вызывать у собеседника определенные эмоции — то есть я могу заставить его чувствовать то, что надо мне. Вот мы и подобрались к объяснению того, почему невербальные сигналы настолько важны.

Когда я собираюсь проникнуть в какое-либо помещение или провести вишинг, то испытываю сильный страх: боюсь провала, опасаюсь, что меня поймают, что допущу ошибку. Давайте разберемся с этой эмоцией.

Как страх влияет на мою физиологию?

- Мои глаза открываются шире, веки напрягаются.
- Рот сжимается, дыхание становится резким.
- Мускулы всего тела напрягаются, и я как бы замираю, инстинктивно готовясь драться или бежать.
- У меня ускоряется сердцебиение.
- Я больше потею.

А теперь разберемся, какие физиологические проявления с моей стороны нужны для того, чтобы получить от объекта воздействия желаемый эмоциональный ответ (легкую грусть, стимулирующую эмпатию):

- Взгляд должен быть мягким, ненапряженным.
- Кончики губ должны быть слегка опущены.
- Мускулы следует расслабить.
- Дыхание должно быть поверхностным.

Большая разница, согласитесь. Если моя легенда предполагает грусть, но язык моего тела будет выражать страх, как отреагирует объект воздействия? Полагаю, он вряд ли подумает буквально: «Этот человек рассказывает грустную историю, но все его поведение свидетельствует о том, что он испытывает страх. От такого несоответствия эмоциональному содержанию мне некомфортно». Однако у него наверняка автоматически сработает внутренний радар, предупреждающий о необходимости держать оборону, потому что с собеседником происходит что-то подозрительное. Если бы я демонстрировал страх, пытаясь вызвать грусть и сочувствие, я бы только отпугнул собеседника.

Необыкновенное исследование под названием «Химикосенсорные ключи конспецифичного стресса активируют у людей миндалевидное тело» (www.ncbi.nlm.nih.gov/pmc/articles/PMC2713432) доказывает это… эээ… интересным образом.

Исследователи собрали образцы пота у людей после выполнения физических упражнений. А затем — образцы пота у людей, которые только что прыгнули с парашютом в тандеме с высоты больше 3000 м. Затем эти образцы давали понюхать испытуемым, которых посадили в аппарат МРТ (да уж, звучит отвратительно).

Когда испытуемые нюхали образцы пота людей, совершивших прыжок с парашютом, в их мозгу активизировался центр страха (та самая миндалина). А когда они нюхали образцы людей, вспотевших из-за занятий спортом, этого не происходило. Получается, что страх в прямом смысле можно «учуять».

А раз окружающие способны «разнюхать» наш страх, как лучше подготовиться к взаимодействию с объектом? Я предлагаю два варианта:

- Научиться контролировать проявления страха, чтобы подавлять их и демонстрировать нужные эмоции.
- Если это невозможно, надо использовать легенду, согласующуюся с моими естественными эмоциями.

ЗАДУМАЙТЕСЬ

На конференции DEF CON 25 наш СИ-подкаст посетил Тим Ларкин. Он рассказал историю о мусульманке, которая проходила мимо группы молодых людей. Они ничего особенно не говорили и не делали, но она почувствовала: здесь что-то не так. И поступила разумно: развернулась и пошла в другом направлении.

Однако женщина была в наушниках и не слышала, что происходит у нее за спиной. Один из молодых людей подбежал к ней сзади и ударил по голове так сильно, что она потеряла сознание.

Эта история — пример того, как работает наш внутренний радар даже в ситуациях, когда ничего откровенно опасного, казалось бы, не происходит. И я всегда советую не заглушать его сигналы, потому что он может спасти жизнь.

Зная это, постарайтесь лучше разобраться в своих эмоциях и понять, что именно показываете окружающим. Вы можете научиться считывать, использовать и правильно реагировать на эмоции и невербальные сигналы объектов воздействия.

И прежде чем мы перейдем к подробному обсуждению невербальных сигналов, я хочу пояснить, что такое базовая эмоция и как ее интерпретировать.

Ваша базовая эмоция работает на нас

Умение считывать эмоции собеседника способно кардинальным образом влиять на ваши коммуникативные компетенции. Поэтому сейчас я хотел бы сосредоточиться на том, как отслеживание изменений базовой эмоции помогает социальному инженеру в работе.

Сразу хочу пояснить, что такое базовая эмоция. Попросту говоря, это то эмоциональное состояние человека, которое вы видите в начале своего наблюдения. То есть не нужно пытаться выяснить, какие эмоции он обычно испытывает, я не призываю вас следить за объектом долгие месяцы перед каждым тестом.

Посмотрите на илл. 8.2. Амайя сделала что-то не очень хорошее, и мама ей об этом сообщает.

Что вы видите? Какую эмоцию демонстрирует моя жена Ариса? Обратили внимание на напряжение в челюсти? Поднятый палец и сжатые губы? Очевидно, она демонстрирует злость.

А что Амайя? У нее сложены руки на груди, поднят подбородок и лицо выражает раздражение. Она закрылась и явно не в настроении слушать обращенные в свой адрес претензии.

А теперь посмотрите на илл. 8.3. Обратите внимание на то, как Амайя выглядит после того, как «обсуждение» закончилось и они с матерью разошлись по разным комнатам.

Амайя выглядит грустной и словно пытается успокоиться. Возможно, вспоминает слова, сказанные в пылу ссоры.

Илл. 8.2. Какие эмоции вы видите?

Илл. 8.3. Что изменилось?

А теперь посмотрите на илл. 8.4. Амайя и Ариса только что выпили по кружке чая и теперь обсуждают, как сходили по магазинам.

Какую базовую эмоцию вы видите здесь? Обе счастливы. Они тянутся друг к другу и явно наслаждаются беседой.

На этих трех фотографиях изображены одни и те же люди в разных условиях, демонстрирующие разные базовые эмоции. И в этом заключается важный для нас урок. Базовая эмоция не связана с личностью человека. Это не элемент его психологического профиля. Это просто эмоциональное состояние, которое он демонстрирует в конкретный момент времени.

Умение считывать эмоциональное состояние человека перед тем, как подойти к нему и заговорить, крайне важно для социального инженера. Чтобы успешно найти общий язык с Арисой на илл. 8.2 и Арисой на илл. 8.4, нужно действовать по-разному.

Илл. 8.4. Какую базовую эмоцию видно по этому снимку?

Я много раз слышал, что можно научиться за считаные секунды определять, врет человек или нет.

Ученые Дэвид Мацумото, Хуи Сун Хуан, Лиза Скиннер и Марк Франк опубликовали статью под названием «Оценка правдивости и выявление обмана» (https://leb.fbi.gov/articles/featured-articles/evaluating-truthfulness-and-detecting-deception), в которой сформулировали очень важную мысль: «Ложь можно определить не только по присутствию или отсутствию каких-либо форм поведения (например, по тому, что человек избегает смотреть вам в глаза или по его беспокойным телодвижениям). Важнее то, как постепенно невербальные сигналы меняются по отношению к базовой эмоции, а также то, как они соответствуют словам, которые

индивид произносит. Анализ поведенческих сигналов позволяет точно определять, врет человек или говорит правду».

Понимаете, что имеют в виду авторы? Нет никакого мистического сочетания действий, увидев которое вы уличите собеседника во лжи. Однако постепенное изменение поведенческих сигналов может указать на то, какие эмоции на самом деле испытывает человек и как их расшифровать.

Остерегайтесь ошибочных толкований

Люди часто придерживаются ошибочных представлений относительно определенных «подсказок» языка тела. От них обязательно нужно избавиться еще до того, как вы начнете заниматься социальной инженерией профессионально. В противном случае вы рискуете допустить множество ложных предположений.

Давайте вместе проанализируем несколько примеров. Взгляните на илл. 8.5. Что вы видите?

На протяжении многих лет сложенные на груди руки было принято считать признаком закрытости. Но это далеко не всегда так. Если изначально поза человека была открытой и он сложил руки уже в процессе знакомства с вами, тогда, возможно, эта интерпретация верна. Но вообще-то многие люди иногда принимают такую позу, потому что она удобна, а не потому, что хотят дистанцироваться от собеседника. Посмотрите на илл. 8.5: руки Амайи сложены на обеих фотографиях, но на ее истинные эмоции указывает не это, а выражение лица и положение головы.

Илл. 8.5. Расстроена Амайя или нет?

А теперь давайте посмотрим на илл. 8.6.

Фотография, к сожалению, этого не передает, но поверьте мне на слово: она очень быстро трясет ногой. Можно ли назвать это движение признаком того, что она собирается солгать? Или ей просто неудобно? Знаете, встречаются люди, у которых ноги все время не на месте — они словно не могут без движения. Опять же, важно обратить внимание, когда это движение начинается и когда заканчивается, и только после этого можно будет судить о его истинном значении. Попробуйте проанализировать илл. 8.6 как единое целое: положение тела Амайи в пространстве, движения ее ноги, то, как она положила руку на шею. Возможно, все указывает на то, что Амайя чувствует себя не в своей тарелке.

Илл. 8.6. Раздражена ли она, собирается ли солгать, холодно ей или комфортно?

Мой сын Колин двигает ногами, как заведенный. Если бы можно было подключить к нему генератор, он бы вырабатывал достаточно электричества, чтобы обеспечить током весь наш дом. И к обману это не имеет никакого отношения: просто он по натуре живчик. А вот пример того, как я использовал эти знания о поведенческих привычках Колина.

— Колин, как прошла вчерашняя вечеринка? Повеселились? — спросил я.

Он, ковыряя носком обуви паркет, ответил:

— Да нормально. Ничего особенного.

Но я знал, что он поссорился со Стюартом, и хотел выведать подробности. Так что я продолжил расспросы:

— Понятно. А кто там был?

Колин перечислил всех присутствовавших, но Стюарта не назвал. Хмм. Тогда я уточнил:

— А, так Стюарт не пришел? Я думал, он тоже будет.

Вдруг нога Колина резко замерла.

— А, ну да, он тоже был, — и нога продолжила ковырять паркет.

— Ммм… И с ним все в порядке?

Колин твердо оперся на ногу и буркнул: «Ага», после чего нога продолжила движение.

То есть индикатором проблемы были не активные движения ноги Колина, а ровно наоборот — их остановка. И после того как я это понял, понадобились считаные секунды, чтобы узнать, что же произошло на самом деле.

Теперь посмотрите на илл. 8.7. Как вы интерпретируете происходящее на этой фотографии?

СОВЕТ ПРОФИ Не пишите о методах, которые используете, чтобы раскусить своих детей, до тех пор, пока они не вырастут и не раскусят вас. Или хотя бы до тех пор, пока вы не перестанете эти методы использовать. В нашей семье принято постоянно мериться проницательностью. Пока что побеждаю я. Если бы мы вели счет, я бы сказал, что соотношение примерно такое: РОДИТЕЛИ — 5 981 387, ДЕТИ — 5.

P.S. Моя дочь не согласна с таким подсчетом баллов и утверждает, что дела обстоят ровно наоборот.

Прикосновения к лицу, почесывания и другие подобные движения могут указывать на ощущение дискомфорта. Однако есть люди, у которых просто что-то чешется. Так что опять же, нужно в первую очередь отслеживать, когда собеседник совершает эти действия и почему.

Илл. 8.7. Комфортно ей или нет?

В этом контексте пример моего сына Колина тоже весьма показателен: он астматик и аллергик, так что его периодически мучит зуд. В период весеннего цветения бедняга постоянно трогает себя и чешется. Понятное дело, его беспокойные телодвижения указывают не на ложь, а на аллергическую реакцию.

Оказаться в ловушке ложных предположений и начать видеть эмоции там, где их нет, очень просто. А «рассмотрев» несуществующие эмоции, вы так или иначе начнете на них реагировать. Но вам же не хочется обращаться с тем, кому просто холодно, как с эмоционально закрытым и черствым человеком? Или думать, что вас обманывают, наблюдая у собеседника всего лишь симптомы разыгравшейся аллергии?

Бороться с этими ошибками несложно: достаточно рассматривать каждую ситуацию как уникальный случай, не ориентируясь на обобщенные суждения, даже если они сформировались у вас при общении с тем же человеком ранее. Делать какие-либо выводы из поведения имеет смысл как минимум после 15–20 секунд взаимодействия.

В вопросах интерпретации языка тела лично я всегда стараюсь сосредоточиться на изменениях, которые произошли в процессе

общения по сравнению с базовой эмоцией. Причем в первую очередь оцениваю, свидетельствуют ли эти изменения об увеличении или уменьшении ощущения комфорта. В книге «Разоблачение социальных инженеров» я много писал о мимике и языке тела, так что если тема вас действительно интересует, рекомендую эту книгу прочесть.

Ну а сейчас моя задача — сформировать у вас базовое понимание того, чем проявления комфорта отличаются от проявлений дискомфорта. Иметь четкое представление о поведенческих индикаторах этих состояний — то же самое, что владеть картой, по которой можно ориентироваться в пространстве общения и определять, на какие именно сигналы нужно обращать особое внимание.

Основные правила

В этом разделе мы поговорим о четырех главных правилах, которые обязательно нужно запомнить, чтобы научиться верно понимать язык тела. Если вы научитесь применять их в своей практике, вас ждут большие перемены.

Не воспринимайте эти правила как математическое уравнение, где у суммы 1 + 2 + 3 + 4 всегда будет одно значение. Они скорее похожи на общие арифметические законы, ориентируясь на которые можно складывать отдельные невербальные сигналы и точно интерпретировать их совокупность в каждом конкретном случае.

Правило 1: главное — «что», а не «почему»

У этого правила вполне однозначный смысл: не стоит проводить параллели между тем, «что» происходит, и тем, «почему», пока не соберете всю необходимую информацию.

На тренингах по восприятию невербальных сигналов я часто начинаю процесс обучения с озвучивания одной простой истины: «Наблюдая, что происходит, вы не всегда можете понять, почему это происходит».

Представьте, что оказались на таком тренинге. И вот я, о чем-то рассказывая, вдруг ловлю ваш взгляд. Вы скрещиваете руки на груди, ваши брови опускаются, челюсть напрягается, но взгляд вы не отводите. Я замечаю ваше напряжение, оно — признак злости или дискомфорта.

Я заключаю, что вас, должно быть, что-то разозлило в моих словах или действиях. Но на самом деле вполне вероятно, что у вас что-то заболело после прошлогодней операции. Или просто беспокоит желудок и вы злитесь. Или самое простое объяснение: вы отвлеклись от лекции и подумали о чем-то, что вас злит.

Так как же мне найти связь между «что» и «почему» в сигналах вашего тела? В седьмой главе мы уже говорили: чтобы это узнать, нужно

задавать правильные вопросы. Однако во время лекции я не могу вдруг остановиться и начать выспрашивать у вас, чего это вы вдруг так нахмурились.

Правило 2: оценивайте совокупность действий

Делая первые шаги в освоении науки воздействия на людей и поняв, что означают отдельные движения тела или выражения лица, можно решить, что вы с блеском освоили эту науку со всеми ее премудростями. Это опасная дорожка. Чтобы понять истинное значение действий человека, обязательно нужно учитывать общий контекст и другие сигналы его тела. Поэтому следите за совокупностью движений, которая соответствует определенным эмоциям.

Представьте себе, например, такую ситуацию. В беседе с супругом вы говорите, что не согласны с его точкой зрения. При этом супруг складывает руки на груди. Обязательно ли это означает, что он злится, хочет отдалиться или вообще не рад вам?

Мыслите шире. Оцените выражение его лица. Оно злое? Изменилось ли положение его бедер и ног, отвернуты ли они от вас? Какие еще действия помогут вам понять, является ли это складывание рук просто движением или частью какой-то значимой эмоциональной истории?

Правило 3: ищите несоответствия

Важно проверять сообщения от собеседника на соответствие между вербальными и невербальными сигналами. Если человек говорит «да», но при этом отрицательно качает головой, на такое противоречие стоит обратить внимание.

Заметив несоответствие информации, получаемой от человека, полагайтесь на невербальные сигналы — правдивыми, скорее всего, будут именно они. Проанализировав совокупность сигналов и несоответствий между вербальной и невербальной информацией, вы сможете максимально приблизиться к пониманию реального смысла сообщений, передаваемых человеком.

Правило 4: внимательно следите за контекстом

Я выглянул из окна своего кабинета и увидел на улице дочку. Она сжалась в комочек, обхватила себя руками, опустила голову. Все это — признаки грусти и дискомфорта.

Все верно, только я не упомянул одну важную деталь: на улице температура около нуля, а она без куртки.

Зная контекст, вы сможете верно интерпретировать происходящее: Амайе просто холодно. Без понимания контекста (погоды) логично было бы предположить, что ей грустно. Чтобы избежать неправильных

интерпретаций, всегда учитывайте контекст ситуации, в которой находится объект наблюдения.

Кроме этих правил, вам нужно ознакомиться с базовой информацией о языке тела. А после этого мы перейдем к подробному обсуждению отдельных эмоций.

Понимание природы невербальных сигналов

Есть ряд базовых принципов, с которыми нужно разобраться, прежде чем вы начнете свой путь в мире невербалики. Они касаются всех людей без исключения и не зависят от их культуры, пола, расы или вероисповедания. Разобравшись с этими принципами, вы сможете понять, как наши тела передают чувства вне зависимости от того, что мы сознательно хотим показать окружающим.

Внешние стимулы поступают в мозг через пять органов чувств (при отсутствии у человека каких-либо телесных повреждений): зрение, обоняние, вкус, осязание и слух. После того как эти сигналы будут обработаны мозгом, он вызовет семь основных эмоций: гнев, страх, удивление, отвращение, презрение, печаль или радость. Эмоции, в свою очередь, вызывают определенную психологическую реакцию, которая выражается в движениях мышц лица и тела.

Например, когда человек ощущает уверенность в себе, он пытается «увеличить» себя в пространстве, в результате чего в его крови повышается уровень тестостерона и снижается уровень кортизола (согласно результатам исследования А. Д. Ноздрачева, А. И. Иванова, В. В. Кирьянова и Р. С. Минвалеева под названием «Постуральные влияния на уровень гормонов у здоровых людей»; https://link.springer.com/article/10.1023/B:HUMP.0000036341.80214.28). Ученые проверяли, как определенные позы йоги влияют на уровни кортизола, тестостерона, дегидроэпиандростерона (ДЭА) и альдостерона. В контексте этой книги нас интересуют в первую очередь кортизол и тестостерон.

Исследователи обнаружили, что пребывание в некоторых позах, связанных с уверенным поведением, повышает уровень тестостерона более чем на 16%, а показатели кортизола снижает на 11%. Тестостерон, в свою очередь, усиливает ощущение уверенности в себе и стимулирует соответствующее поведение. Получается своего рода исполнение желаний: вы хотите быть увереннее, принимаете соответствующую позу — и в кровь выделяются вещества, которые помогают вам чувствовать и вести себя уверенно.

ЗАМЕТКА Кортизол — гормон, который регулирует широкий спектр процессов, происходящих в теле, в том числе метаболизм и иммунный ответ. Из-за связи кортизола со стрессовыми реакциями его часто

называют «гормоном стресса». Повышенный уровень кортизола сопровождает тревожные расстройства и депрессии.

Крайне важно понять следующее: судя по всему, связанные с ощущением комфорта невербальные сигналы способствуют появлению химических и психологических реакций счастья, уверенности и силы. В то же время невербальные сигналы, возникающие при дискомфорте, провоцируют возникновение стресса, тревоги и других реакций, связанных с негативными эмоциями.

И нужно разобраться, как определенные невербальные сигналы действуют на вас и на объект воздействия — ведь профессиональный социальный инженер влияет на эмоциональное состояние объекта (или манипулирует им). Относиться к этому следует серьезно.

Легенда может производить на объекты воздействия как краткосрочный, так и долгосрочный эффект, поэтому планировать его нужно тщательно и осторожно. Не забывайте мантру: после общения с вами люди должны чувствовать себя лучше, чем до него. Если это возможно, старайтесь использовать легенды, вызывающие эмоции, которые не будут оказывать долгосрочного негативного влияния на взаимодействующих с вами людей.

Как оценить риск возникновения такого долгосрочного негативного эффекта? Для начала определите, на какой эмоции основывается ваша легенда. Страх, гнев, отвращение и презрение — сильные негативные эмоции, используя которые вы рискуете навредить объекту воздействия.

Например, оцените различия между эффектом фишинговых сообщений следующего содержания: «Мы благодарим вас за заказ 55-дюймового телевизора» и «Ваш аккаунт взломали, а банковский счет опустошили».

Осознание, с какой силой невербальные сигналы и эмоции влияют на собеседника, поможет вам определиться, как именно использовать эти эмоции в своей работе. В этом смысле один из главных уроков, которые можно вынести из трудов Пола Экмана, заключается в том, что эмоции вызывают определенные невербальные реакции, но работает этот механизм и в обратную сторону. Эта идея подтверждается в многочисленных научных исследованиях. К их числу относится работа под названием «Условия торможения и фасилитации улыбки у людей: Проверка гипотезы мимической обратной связи без навязчивого вмешательства» (Inhibiting and Facilitating Conditions of the Human Smile: A Nonobtrusive Test of the Facial Feedback Hypothesis) (https://www.ncbi.nlm.nih.gov/pubmed/3379579). Страк, Мартин и Степпер проверили гипотезу, которую Экман сформулировал еще в 1970–1980-х годах, и показали, что, моделируя определенное выражение лица, можно вызвать соответствующую ему эмоцию. Проверяли они это следующим образом: просили испытуемых зажать во рту ручку, тем самым стимулируя мускулы, задействованные в улыбке. В итоге они получили такие же результаты, как и доктор Экман в своих исследованиях:

имитация выражения лица (даже принудительная) вызывает возникновение связанной с ней эмоции.

Так что помните: если вы провоцируете эмоцию или каким-то образом заставляете собеседника ее демонстрировать, вполне возможно, что в результате он ее действительно ощутит. Используйте эту сверхспособность с особой осторожностью.

Комфорт и дискомфорт

Социальный инженер должен уметь эффективно общаться, а невербальная коммуникация представляет собой неотъемлемую часть любого общения. Исследователи по-разному оценивают процент невербалики в нашем общении. Я слышал о 80, 85 и даже 90%. Однако благодаря Полу Экману я понял, что, хотя невербальные сигналы действительно сильно влияют на общение, форма этого общения (устная, письменная, личная), в свою очередь, влияет на невербалику.

Сигналы, передаваемые через тело и лицо в процессе нормального общения, способны дать людям, умеющим их интерпретировать, огромное количество полезной информации. Кого-то такой поток может сбить с толку. Поэтому в начале вашего социально-инженерного пути рекомендую сосредоточиться на невербальных сигналах, которые интерпретировать проще всего, а именно на признаках комфорта и дискомфорта.

В этой книге я попытаюсь сделать то, чего не делал ни в одной из предыдущих: начну с обсуждения эмоций, а после мы разберемся, как вызывать эти эмоции у объектов воздействия с помощью социальной инженерии. Я объясню, какие признаки указывают на состояние комфорта или дискомфорта, связанного с каждой эмоцией. Глава поделена на подразделы в соответствии с основными эмоциями. В каждом из подразделов я опишу формы проявления этих эмоций в языке тела и мимике. Конечно, исчерпывающего списка всех возможных движений вы здесь не найдете. Но мои примеры можно использовать как базу для дальнейшего накопления знаний по мере приобретения профессионального опыта и освоения навыка «чтения» невербалики.

Чтобы научиться понимать истинное значение языка тела другого человека, нужно также разобраться и с тем, как ваш язык тела способен повлиять на объект воздействия. Если вы демонстрируете какую-либо эмоцию из описанных в этом разделе, та же эмоция может возникнуть и у собеседника. Определитесь, какие чувства вам надо вызвать у человека, а затем поработайте над воспроизведением соответствующих им невербальных сигналов. Кроме того, научитесь определять эмоции и действия, возникновение которых не следует провоцировать у других людей.

Гнев

Гнев просто сокрушительная эмоция, способная привести к возникновению новых чувств и совершению опасных действий: от использования ненормативной лексики или злых выражений до проявления физической агрессии.

На физиологическом уровне из-за гнева мы напрягаемся, готовимся нападать или защищаться. Мускулы напряжены, челюсти стиснуты, кто-то сжимает кулаки — все признаки готовности ринуться в бой. Когда обстановка совсем уж накаляется, некоторые даже инстинктивно опускают подбородок, как бы защищая шею.

В то же время, когда люди злятся, они стараются занять больше места в пространстве, выглядеть крупнее: расправляют грудную клетку и плечи, шире расставляют ноги. Дыхание становится глубже, пульс учащается.

В лице человека, испытывающего гнев, наблюдаются следующие изменения:

- Брови сдвигаются, но глаза открыты широко, не щурятся.
- Челюсть напряжена.
- Зубы сжаты, а если рот открыт, то из него зачастую вылетают весьма неприятные слова.

Все это изображено на илл. 8.8.

Илл. 8.8. Гнев в мимике

Злость выражается не только в лице, но и в теле. На илл. 8.9 я сжал челюсти и кулаки. Кроме того, у меня грудь колесом — чтобы показаться потенциальному противнику крупнее. Все это указывает на гнев (чтобы вы знали, именно с таким видом я встречаю мальчиков, которые

проявляют интерес к Амайе). Если, подходя к объекту воздействия, вы заметите эти признаки, вероятно, с этим человеком лучше пока не связываться.

Еще один вариант выражения умеренного гнева демонстрирует Амайя. На эту эмоцию указывают ее колючий взгляд, сжатые челюсти и нахмуренные брови.

Илл. 8.9. Гнев в теле

Илл. 8.10. Легкое раздражение

В большинстве случаев невербальные признаки гнева связаны с ощущением дискомфорта. Вызывать эту эмоцию у объектов воздействия я не люблю. Поэтому отслеживаю ее проявления у себя и стараюсь в процессе работы ее не демонстрировать.

Тем не менее если я выбираю слишком агрессивный подход или слишком негативную легенду, в невербальных сигналах объекта воздействия зачастую проскальзывают признаки гнева. Это явный сигнал того, что нужно немного сбавить обороты, смягчить голос и язык тела, чтобы не подпитывать гнев собеседника.

Отвращение

Отвращение еще одна сильная эмоция. Ее можно испытывать по отношению к человеку, месту или вещи. Если что-то заставило нас ощутить сильное отвращение, мы помним это долгое время.

Когда я был маленьким, мои родители выращивали кур. Я часто бегал в курятник, брал оттуда пару свежих яиц и готовил блюдо, которое мы называли «яйцо в хлебе»: жарил на сковородке в масле два куска хлеба и разбивал между ними яйцо.

И вот однажды я, как обычно, принес яйцо, разбил его на сковороду… но вместо желтка из яйца вывалился полусформировавшийся цыпленок. Упав на раскаленную поверхность, он подергался и умер. Это зрелище и запах заставили меня буквально отпрыгнуть в сторону. Отвращение было настолько сильным, что я убежал, забыв выключить конфорку, и трупик бедного создания продолжал жариться, наполняя кухню запахом сгоревшей курицы.

Сила этой эмоции давала о себе знать даже десять лет спустя: мне становилось плохо от одного только запаха яичницы. Впрочем, постепенно мне удалось преодолеть это ощущение. Социальные инженеры должны осознавать силу отвращения. Если объект воздействия почувствует его по отношению к вам, восстановить репутацию в его глазах уже вряд ли удастся.

Подумайте, что может заставить вашего собеседника испытать отвращение: запах тела и определенные физиологические проявления, застрявший у вас в зубах кусочек пищи, нецензурная лексика, жесты и т.п. Заранее анализируйте свои действия и внешний вид, чтобы этого не произошло.

Выражаться отвращение может по-разному. На лице эта эмоция отражается билатерально, то есть симметрично (см. илл. 8.11).

Когда мы снимали иллюстрации для этой главы, собака сделала кое-что неприятное прямо у нас в гостиной. Я не мог упустить такой шанс и запечатлел выражение лица Арисы в момент, когда она убирала последствия собачьей выходки. Обратите внимание, как подняты крылья ее носа: тем самым несколько блокируется обоняние и уменьшается угол обзора. Ариса на физиологическом уровне пытается оградить себя от того, что вызвало у нее отвращение.

Илл. 8.11. Отвращение

Теперь о языке тела. Обычно отвращение выражается в попытке отвернуться или отстраниться, поэтому ищите признаки потери интереса и отторжения.

Обратите внимание на положение ног Амайи на илл. 8.12. Что ее интересует в данный момент? Не папа, это очевидно (и обидно, да). И

хотя явное отвращение она не демонстрирует, язык ее тела указывает на дискомфорт и отсутствие интереса.

На мой взгляд, отвращение — эмоция слишком сильная, чтобы использовать ее в работе. Тем не менее иногда меня спрашивают, можно ли провоцировать ее возникновение, чтобы сформировать группу людей, объединенных объектом общей нелюбви. Действительно, такой прием может сработать эффективно. Но при неудачном стечении обстоятельств результаты могут оказаться опасными.

Илл. 8.12. Отсутствие интереса

Презрение

Презрение — эмоция уникальная. Оксфордский словарь английского языка определяет презрение как «ощущение никчемности другого человека». Пол Экман использует более простое определение: он считает, что презрение представляет собой ощущение морального превосходства.

Получается, что презрение можно испытывать только по отношению к человеку. Интересно, что выражается эта эмоция обычно с одной стороны лица: например, в ухмылке, даже напоминающей улыбку (см. илл. 8.13).

Есть одна особенность, характерная для презрения: уголки губ поднимаются только с одной стороны лица, а иногда в ту же сторону слегка смещается и подбородок.

Илл. 8.13. Презрение можно спутать с радостью

Так как презрение связано с ощущением собственного превосходства над другим человеком, оно способно повлечь за собой гнев. Проявляться это может в следующих телесных сигналах:

- Ощущение превосходства заставляет нас чувствовать себя увереннее. Эта уверенность проявляется по-разному, однако обычно она выражается стремлением занять больше места в пространстве.
- Если презрение в итоге разозлит собеседника, то до того, как вы увидите невербальные проявления гнева, можно заметить легкое напряжение челюсти и изменение позы в сторону большей агрессивности.

Я считаю, что использовать презрение в социальной инженерии не стоит. При этом понятно, как его применяют на более масштабном уровне, например в террористических организациях для привлечения новых адептов. Однако социальный инженер едва ли сможет использовать презрение для достижения своих целей.

ЗАМЕТКА Террористические организации часто эксплуатируют также и гнев, который граждане испытывают по отношению к идеологии или к правительству страны, и стремятся трансформировать этот гнев в презрение. Когда объект воздействия ощущает презрение (то есть свое моральное превосходство по отношению к объекту, на который направлен гнев), террористы предлагают «решение» и подсказывают, какие «действия» нужны для улучшения ситуации. Поразительно, как эффективно этот метод работает для разделения людей на воинствующие группы.

Страх

Страх — интересная эмоция. Цели у него могут быть совершенно разными: обычно он предупреждает нас об опасности, но в контролируемых дозах может даже веселить. Некоторым людям ощущение испуга или страха доставляет явное удовольствие.

Боязнь разочарования, неудачи, принятия неверного решения со стороны объекта воздействия, конечно, помогает социальному инженеру. И тем не менее использовать страх в больших количествах все же не стоит. Легенды, откровенно угрожающие объекту или пугающие его (например, потерей работы, семьи, жизни), могут вызвать слишком сильные эмоции. Если позже человек узнает, что его заставили все это переживать ради проверки безопасности, он наверняка испытает отвращение, презрение и гнев.

На уровне мимики страх выражается следующим образом:

Глаза широко открыты, мы стремимся максимально увидеть происходящее.

Тело напрягается, как правило, мы тяжело дышим.

Рот приоткрыт, губы растянуты, словно человек беззвучно кричит: «И-и-и!».

Все это наглядно изображено на илл. 8.14.

Илл. 8.14. Страх в его классическом выражении

Что касается языка тела: испуганный человек, скорее всего, отпрянет, напряжется, поежится. Его поза будет выражать готовность бороться или убежать. Если вы испугаете собеседника, то, скорее всего, увидите реакцию как на илл. 8.15.

Обратите внимание на то, как Амайя отпрянула и напряглась всем телом. Ее рот растянут в беззвучном «и-и-и!». Она сидит в кресле и бежать ей некуда, что, скорее всего, только усиливает ощущение страха.

Илл. 8.15. Язык тела выражает испуг

На илл. 8.16 изображено еще одно движение, которое часто совершают испуганные женщины, — попытка прикрыть яремную ямку.

Илл. 8.16. Если человек прикрывает яремную ямку, он боится

Обращайте внимание на неявные телесные индикаторы эмоций: они помогут разобраться в чувствах объекта. Заметив признаки страха, вы сможете решить, насколько эта эмоция уместна и потенциально эффективна в конкретном контексте. Как я уже говорил выше, использовать страх в социальной инженерии можно, но я стараюсь не создавать ситуаций, в которых объекты будут чувствовать себя действительно в серьезной опасности.

Удивление

Удивление часто путают со страхом, потому что выражаются они похожим образом: глаза удивленного человека открыты широко, тело замирает, рот приоткрывается. Однако его взгляд не испуган, а рот приоткрыт скорее как при произношении звука «о», а не «и» (см. илл. 8.17).

Социальный инженер может эффективно использовать удивление. Однако, как и с уже описанными эмоциями, все зависит от конкретной ситуации. Я не рекомендую неожиданно выпрыгивать из шкафа, чтобы вызвать у человека удивление. А вот легенда, подразумевающая неожиданную проверку или награду, зачастую вызывает как раз

подходящую реакцию. В ходе одной операции, полностью основанной на вишинге, я с большим успехом использовал неожиданное поощрение.

Объект: Добрый день, Бэт у телефона. Чем я могу помочь?

Я: Бэт, меня зовут Пол, я из отдела управления персоналом. У меня для вас отличные новости. Возможно, вы еще не в курсе, но ваше отделение участвовало в розыгрыше нового iPhone и удача выпала именно вам!

Илл. 8.17. Удивление, которое часто путают со страхом

Объект: Да ладно?! Вы шутите? Это так радостно!

Я: Понимаю. Обожаю обзванивать победителей. Повезло десяти участникам, и мне нравится быть вестником добрых новостей.

Объект: Да уж, а ведь я ничего никогда не выигрывала! Вот вы меня удивили!

Я: Представляю. Но в компании у нас работает несколько сотрудниц по имени Бэт, поэтому мне нужно проверить некоторые детали, чтобы убедиться, что вы — правильная Бэт. Уточните, пожалуйста, как пишется ваше полное имя.

Объект: Э-л-и-з-а-б-е-т С-м-а-р-т-с-о-н.

Я: Все верно. Теперь назовите, пожалуйста, свой идентификационный номер сотрудника, чтобы я мог внести его в систему.

Объект: Т238712Р.

Я: Ну вот, отлично, вы — та самая Бэт. Сейчас дам вам сайт, где нужно зарегистрироваться и написать адрес, по которому будет доставлен телефон. Наберите в браузере айфон.название-компании.com. [Сайт был сделан нами заранее, и ни одна кнопка на нем не работала.]

Объект: Так, зашла на сайт, вижу логотип, но, когда жму на кнопку «Войти», ничего не происходит.

Я: Странно. У меня он тоже сейчас открыт. Так, что происходит, когда вы жмете на «Войти»? Я сразу попадаю на следующую страницу.

Объект: Нет. Сейчас попробую другой браузер. [Перепробовала все установленные на компьютере браузеры.] Ну да, как обычно. Что-то выиграла и теперь не смогу получить.

Я: Ну уж нет, так не пойдет. Хотите, я внесу нужную информацию?

Объект: А вам не сложно?

Я: Никаких проблем. [Здесь я уже чувствовал себя очень виноватым.] Значит, сначала нужно ввести полное имя, его я знаю. [Нажимаю на клавиши, будто вбиваю ее имя в форму.] Так, жму «Дальше». Опять спрашивает номер сотрудника, его вы тоже мне уже сказали.

Объект: Боже мой, спасибо вам огромное.

Я: Хорошо. Теперь нужен ваш логин. Полагаю, Э. Смартсон?

Объект: Вообще-то Б. Смартсон, от Бэт.

Я: Ага, понял. И последнее — осталось ввести пароль.

Объект [ни на секунду не задумываясь]: Пароль у меня хороший, длинный. JustinandBeth99!

Я: Отлично, все в порядке, регистрация прошла успешно. Здесь говорится, что в течение суток вы получите электронное письмо с дальнейшими указаниями о том, как получить смартфон. Поздравляю вас, Бэт!

Объект: Спасибо!!!

После этого вся Сеть оказалась под ударом. Да, это была манипуляция (так и вижу, некоторые читатели начинают тихо меня ненавидеть), и, когда она раскрылась, Бэт, конечно же, расстроилась. Но обратите внимание: я ничем ей не угрожал, не стыдил, никак ей не навредил. Я только использовал ее удивление для пробуждения эмоций, связанных с радостью, и в результате девушка, не задумываясь, выдала мне много персональной информации.

Если вернуться к теме языка тела, то удивление обычно выдают действия, изображенные на илл. 8.18 и 8.19.

Я рекомендую социальным инженерам использовать удивление в работе. Если правильно планировать и воплощать воздействие на человека этой эмоции, можно добиться больших побед.

Илл. 8.18. Удивленный человек может немного отклониться назад и всем телом как бы приподняться вверх

Илл. 8.19. Шок, как крайняя форма удивления, может выражаться в жесте закрывания рта рукой

Печаль

Печаль — эмоция очень сложная. Ее диапазон простирается от легкой меланхолии до глубокого отчаяния. Социальный инженер может использовать печаль несколькими способами:

- замечать ее проявления в невербалике объекта и использовать для получения определенной реакции;
- моделировать ситуации, которые с большой вероятностью заставят объект воздействия ощутить грусть и повести себя удобным для вас образом;
- самому демонстрировать грусть через невербальные сигналы, чтобы вызвать у объекта эмпатическую реакцию.

Да, некоторые из перечисленных методов предполагают манипуляции. Но большое значение имеет то, как именно вы собираетесь использовать эти эмоции и в каком эмоциональном состоянии окажется человек, на которого вы будете воздействовать.

Илл. 8.20. Мимическое выражение грусти

Можно выделить несколько мимических индикаторов грусти (см. илл. 8.20):

- уголки губ опущены;
- веки прикрыты;
- брови сдвинуты и приподняты вверх

Кстати, иногда печаль можно «считать», даже если вы видите только часть лица.

Грусть выражается и в языке тела: мы пытаемся защититься, успокоить себя, стать меньше. Это состояние полностью противоположно ощущению уверенности.

Примеры демонстрации потребности себя утешить на уровне языка тела изображены на илл. 8.21, 8.22 и 8.23.

Илл. 8.21. Чтобы успокоиться, можно себя приобнять

Илл. 8.22. Глаза отведены в сторону

Список получился короткий, но, думаю, у вас уже сложилось представление об основных аспектах. Если заметите у собеседника эти невербальные сигналы, можете смело делать вывод о том, что он испытывает дискомфорт.

При всей своей сложности печаль считается весьма полезной для социального инженера эмоцией — причем как при считывании, так и при использовании по условиям легенды. Однако призываю вас обращаться с этой эмоцией осторожно.

Мне не хочется, чтобы после встречи со мной людей переполняла печаль или чтобы они переживали горе. Однако легкая грусть способна вызвать у человека сильную эмпатическую реакцию. Йорг Барраза и Пол Зак в своем исследовании под названием «Эмпатия по отношению к незнакомцам способствует выделению окситоцина и проявлению щедрости» (https://nyaspubs.onlinelibrary.wiley.com/doi/abs/10.1111/j.1749-6632.2009.04504.x) продемонстрировали, что уровень окситоцина повысился на 47% после того, как испытуемый ощутил эмпатию по отношению к совершенно незнакомому человеку. В то же время печаль связана со снижением уровня серотонина, дофамина и окситоцина в мозгу. Поэтому в работе я стараюсь использовать печаль именно как инструмент, провоцирующий возникновение эмпатии. Но всегда избегаю ситуаций, в которых объект воздействия будет вынужден ощутить беспокойство, скорбь и другие депрессивные эмоции.

Илл. 8.23. Надломленная поза

Просто подумайте о том, как часто эту тактику используют маркетологи и представители благотворительных организаций. Фото несчастных детей и бездомных животных должны вызвать у вас эмпатическую реакцию и подтолкнуть к решению отдать свои деньги. Причем речь не обязательно идет про обман и манипуляции. Просто люди знают, как работает мозг человека, и используют это знание для достижения своих целей.

Радость

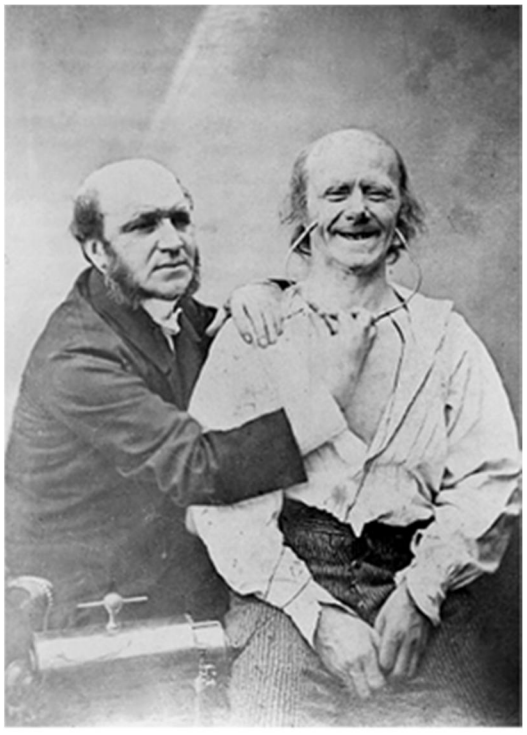
Наверняка все единодушно согласятся с тем, что радость — очень полезная в процессе общения эмоция. Когда нам радостно, мы довольны, расслаблены и легче принимаем альтруистические решения. Нам нравятся люди, места и вещи, которые нас радуют.

Понятно, почему социальным инженерам так важно научиться считывать и вызывать у людей радостные эмоции. И первый навык, который послужит вам на этом пути, — умение отличать искреннюю улыбку от фальшивой. Главный критерий в этом процессе — активация круговой мышцы глаза. Именно она отвечает за подъем щек и специфические морщинки вокруг глаз («гусиные лапки»).

В середине XIX века французский исследователь Дюшен де Булонь показал, что искреннюю улыбку можно имитировать. Он проводил неврологические эксперименты с инвазивными формами электрошока: так ученый стимулировал необходимые мышечные движения (https://www.thevintagenews.com/2016/05/07/44782-2/).

Поскольку его эксперименты были болезненными, исследования далеко не продвинулись. Но именно Дюшен де Булонь доказал, что мышцы лица представляют собой средство прямого выражения эмоций. В 1855 году он разработал метод стимуляции мышечного ответа током. А затем описал этот опыт в своей книге «Механизм человеческой мимики» (Mécanisme de la physionomie humaine). Пример такой стимуляции изображен на илл. 8.24.

Результаты этого исследования помогают понять, почему радость обычно вызывает у нас улыбку. Однако профессиональному инженеру нужно научиться различать и другие невербальные проявления радости.



Илл. 8.24. Фальшивая «искренняя» улыбка

Так как же радость выражается на языке тела? Мы знаем, что она способствует выделению в кровь определенных химических веществ, она отвечает за ощущение уверенности. Значит, можно смело предположить, что все это будет определенным образом выражаться и в

языке тела. Позы, связанные с ощущением радости, изображены на илл. 8.25, 8.26 и 8.27.

ЗАМЕТКА У всех животных самой уязвимой частью тела считается живот, поэтому его демонстрация воспринимается как жест доверия. У людей этот сигнал передается через раскрытие кистей, яремной вены и других частей тела, которые инстинктивно хочется защищать во время нападения.

Илл. 8.25. Обратите внимание на открытость и уверенность, отражающуюся в положении рук

Илл. 8.26. Раскрытая кисть — признак доверия и радости

Если говорить о мимике, то кроме рта в улыбке должны быть задействованы глаза. Что касается улыбки, она может быть открытой и закрытой (см. илл. 8.28). Испытывая радость, мы обычно наклоняемся ближе к объекту, который это чувство у нас вызвал.

К признакам радости также можно отнести подпрыгивания или вставание на цыпочки. Когда мы чувствуем себя уверенно или хорошо, мы не стесняемся занимать пространство вокруг себя, а потому больше двигаемся.

Радость я использую в работе очень часто. Обращение к эго человека позволяет вызвать у него радостные ощущения и подтолкнуть к принятию эмоционального решения. Но чтобы такой заход сработал, это обращение должно быть реалистичным, правдоподобным и соответствовать уровню уже установившегося между нами раппорта.

Илл. 8.27. Открытая ладонь зачастую ассоциируется с гостеприимством или сердечным приветствием

Мой опыт показывает, что люди чувствуют себя в моей компании намного комфортнее, если я подхожу к ним с раскрытыми ладонями, тепло улыбаюсь и при этом наклоняю слегка голову (конечно, все эти действия не должны противоречить легенде).

Ищите возможность моделирования радостного окружения для объекта воздействия через легенду — и наверняка получите хорошие результаты.

Илл. 8.28. Радость на лице: искренняя улыбка и легкий наклон головы

Резюме

Невербальные сигналы — большая и сложная тема, которую нельзя охватить в одной короткой главе. Выше я уже выражал надежду на то, что, изучив эту информацию, вы найдете в ней приемы для пополнения своего профессионального арсенала. Понимание механизма функционирования эмоций усовершенствует любую легенду. И чем лучше вы будете понимать, что вам без слов сообщает другой человек, тем яснее осознаете истинный смысл того, что говорят вам вслух. Мне хотелось бы, чтобы из этой главы вы вынесли следующее:

Основополагающие инструменты. Надеюсь, вы сориентировались в изобилии сигналов, с помощью которых мы передаем эмоции мимикой и языком тела.

Более полное понимание. Хочется верить, что теперь вы лучше понимаете, какие эмоции могут помочь в работе, как считывать проявления этих эмоций у других людей и самим демонстрировать их.

Защита. Понимание того, как эмоции выражаются через мимику и жесты, может пригодиться вам для защиты от злоумышленников. Узнав, как использовать невербалику для влияния на человека, вы научитесь распознавать и ситуации, когда ее будут пытаться использовать против вас.

Улучшение. Профессиональный социальный инженер должен постоянно учиться и все время расширять набор доступных ему навыков.

Мне хочется рассказать вам еще одну историю, которая поможет закрепить в памяти информацию, собранную в этой главе. На

конференции DEF CON мне довелось пообщаться с сотрудником одной организации, и он наглядно продемонстрировал мне, насколько это важно — всегда помнить о невербалике.

Обычно на этой конференции мы с моей командой постоянно чем-то заняты. Я работаю практически без перерывов, даже пары минут себе не уделяю. Просто тружусь в режиме нон-стоп, подпитываясь энергией и позитивом от толпы посетителей.

Я люблю это состояние, хотя в нем трудно понимать чувства окружающих. Бегаю туда-сюда, раздаю указания и слежу за тем, чтобы все шло как по маслу. Так вот, однажды я попросил нескольких сотрудников кое-что упаковать. Шел последний день мероприятия, и мы очень спешили собраться, чтобы пойти всей командой на прощальный ужин в наш любимый японский ресторан.

Все шло нормально, я бы даже сказал, на 100% идеально. Оставалось провести церемонию закрытия — и можно было наконец-то расслабиться. Но когда я вдруг задумался о том, что сейчас чувствуют члены моей прекрасной команды, то заметил на лице одного из них даже не усталость, а настоящее изнеможение. А у другой — мучения и боль.

Первому я сказал:

— Слушай, если ты совсем умотался, можешь отпроситься с церемонии закрытия.

— Серьезно? Можно просто не приходить?

— Да, конечно. Я думал, это и так понятно.

— А я понятия не имел, что можно уйти. Думал, присутствовать обязательно.

— Только для Мишель. Все остальные при желании могут уйти.

Услышав это, сотрудник выдохнул с облегчением.

Подходя к другой сотруднице, я понял, что нужно действовать деликатнее. Нельзя просто окликнуть ее и при всех расспрашивать, потому что на лице у нее отражалась смесь грусти, злости и страха — а значит, случилось что-то серьезное.

Я улучил момент, когда можно было тихонько отозвать ее в сторонку, и спросил, все ли у нее в порядке. Не буду описывать, что именно происходило дальше — но слез пролилось много. Оказалось, она сильно переживала из-за того, что некоторые задачи приходилось бросать не доделав. И буквально валилась с ног от усталости.

Тогда я сделал очень важные для себя выводы. И на протяжении последнего дня конференции внимательно наблюдал за эмоциями членов моей команды (конечно, об этом стоило подумать намного раньше, до того как ситуация стала критической).

К социальной инженерии это имеет прямое отношение. Будьте наблюдательными не только во время выполнения заданий. При поиске «флагов» не забывайте и о наблюдательности в процессе общения. Следите за изменениями базовой эмоции объекта воздействия. Это поможет разобраться в том, что человек чувствовал до, в процессе и после взаимодействия с вами.

Умение читать невербальные сигналы — навык действительно эффективный. А если вы научитесь использовать невербалику с тем, чтобы вызвать у объекта определенные эмоции, то просто вознесетесь до уровня супергероя.

На этой прекрасной ноте я и закончу главы, посвященные навыкам, необходимым в работе социального инженера. Дальше мы обсудим, как применять их в ходе пентестов. При каких векторах атаки они применимы? Разберемся в следующей главе.

9

Взлом сознания

> Если деньги — ваша надежда на независимость, то вы никогда не станете независимым. Единственная настоящая гарантия, которую человек может получить в этом мире, — это запас его знаний, опыта и возможностей.
>
> Генри Форд

В предыдущих главах я описал изменения, произошедшие в сфере социальной инженерии за последние семь лет: в методах сбора данных из открытых источников и их использовании, в моделировании коммуникации, легендировании, установлении раппорта, влиянии, манипуляциях, извлечении информации и трактовке невербальных сигналов. Получилась отличная база знаний с точки зрения развития коммуникативных навыков. Но я же профессиональный социальный инженер, а значит, не могу не рассказать, как применять все эти знания в практике СИ.

Преступники и мошенники обычно используют четыре вектора атаки: фишинг, вишинг, СМС-мошенничество и имперсонацию. Для пущей эффективности их могут комбинировать.

В этой главе мы разберемся, как использовать коммуникативные навыки в контексте каждого из перечисленных векторов. Затем я изложу свои соображения по горячо любимой всеми теме составления отчетов (обещаю, буду краток). И наконец, расскажу, как вообще попасть в этот бизнес и привлечь клиентов.

Однако прежде всего нам необходимо обсудить принципы пентестинга. Они должны лечь в основу любой вашей работы в роли социального инженера.

ОБРАТИТЕ ВНИМАНИЕ В этой главе я не говорю о том, как использовать перечисленные навыки в мошеннических целях. Книга

написана для тех, кто хочет стать специалистом в сфере безопасности: социальным инженером, после общения с которым люди будут чувствовать себя лучше, чем до этого общения. Если же эти навыки используют преступники, стремящиеся навредить своей жертве, то о состоянии объекта воздействия они, конечно же, не задумываются.

Перед социальной инженерией все равны

Сразу хочу подчеркнуть, что социальную инженерию можно применять не только к простакам и дуракам. Ее методы действуют на всех нас. Если подобрать правильное эмоциональное воздействие, осуществить его в правильной ситуации с использованием правильной легенды, то в роли жертвы сможет оказаться любой.

Меня часто спрашивают, попадался ли я сам на удочку социальных инженеров-мошенников. К сожалению, попадался. Грамотное эмоциональное воздействие, осуществленное в правильное время, заставили меня купиться на фишинг. К счастью, я отделался легко, но потом было стыдно. Впрочем, мне повезло: я знал, как действовать, чтобы быстро нивелировать последствия. У меня был ПМиП (которому посвящена вся десятая глава этой книги).

Я не любитель слоганов в духе «Нет пределов человеческой глупости». Понятное дело, многие проблемы, связанные с обеспечением безопасности, возникают вследствие лени, а иногда и действительно глупости. Но это вовсе не значит, что мошенники способны обмануть только дураков.

Например, однажды на пресловутое «нигерийское письмо» повелся университетский профессор. Причем он поверил мошенникам до такой степени, что не только опустошил семейный бюджет, но и залез в университетскую казну. Даже после того, как его поймали с поличным и за дело взялось ФБР, профессор обвинял федеральных агентов в желании забрать его деньги и самим поживиться миллионами, которые вот-вот перечислят на его счет.

ОБРАТИТЕ ВНИМАНИЕ «Нигерийские письма» (они же «схема 419») получили свое название благодаря нигерийскому закону по борьбе с мошенничеством. Обычно эти письма начинались с фразы в духе «Я наследный принц с состоянием в миллионы долларов…», хотя в последнее время все чаще пишутся от лица попавшей в беду вдовы. В любом случае эта схема продолжает работать на людях, которые надеются получить огромную прибыль за небольшое вложение.

Согласитесь, глупый поступок. Но это — легкий ответ для тех, кто не хочет разбираться в деталях. Я же предлагаю проанализировать все обстоятельства в целом и подумать о том, что заставило профессора так упорно продолжать верить мошенникам:

- Он столкнулся с серьезными денежными трудностями, а мошенники дали ему надежду на финансовую свободу.
- Когда профессор увидел огромные суммы, которые должны были в итоге оказаться на его банковском счете, им овладела жадность.
- Однажды вложившись, он хотел быть последовательным и не противоречить принятым ранее решениям.
- Он был уверен, что помогает жителю страны третьего мира, а заодно и себе.

Если смотреть на ситуацию с этой точки зрения, несложно понять, почему профессор поверил в мошенничество, которое разрушило его жизнь, пошел на воровство и даже обманул жену. Он руководствовался надеждой, жадностью и желанием оставаться последовательным, помогая другому человеку и себе.

Уже и не сосчитаю, сколько раз руководители разных уровней заявляли, что ни за что не поведутся на мой «развод» — и сколько раз потом злились на самих себя за слив информации, необходимой для получения удаленного доступа в ходе пентеста. Жертвой атаки может стать любой человек, вне зависимости от положения в корпоративной иерархии.

Принципы пентестинга

Пентестинг (или тестирование на проникновение) заказывают компании, желающие проверить, насколько их корпоративная сеть защищена от посягательств профессиональных взломщиков. Главная цель подобных мероприятий — выявить существующие в системе проблемы и найти для них решение до того, как уязвимостью воспользуются реальные преступники.

Со временем пентестинг превратился в стандартный инструмент обеспечения безопасности, и отделы корпоративного регулирования во многих компаниях требуют проводить подобные проверки ежегодно. Однако законов, которые требовали бы использования социальной инженерии в ходе пентестинга, на государственном уровне сейчас существует немного.

Поэтому компании, стремящиеся просто поставить галочку в графе «проверка безопасности», обычно оказываются не лучшими клиентами. Они заказывают проверки, повинуясь требованиям, а не потому, что видят необходимость подобных мероприятий. Как дети, которые убирают за собой на кухне не потому, что любят чистоту или хотят вас удивить, а потому, что вы их заставили.

Существует несколько утвержденных стандартов в отношении пентестинга, а также ряд нормативных требований, на основе которых пентестеры могут подобрать подходящие практики для решения профессиональных задач. В 2009 году я начал разрабатывать системный подход к пониманию социальной инженерии (своего рода СИ-

фреймворк), который и лег в основу ресурса https://www.social-engineer.org/. В настоящий момент многие организации по всему миру используют эту систему для описания оказываемых в ходе пентестинга услуг. И несмотря на это, нельзя сказать, что стандарты социальной инженерии разработаны и утверждены. Думаю, в первую очередь это связано с динамической природой социальной инженерии, из-за которой практически невозможно заранее распланировать все аспекты воздействия на людей.

Тем не менее можно выделить определенные фазы, из которых состоит любая социально-инженерная атака (см. схему на илл. 9.1).

Информация — важнейшая часть любой такой атаки, поэтому первый шаг — это всегда сбор данных из открытых и иных источников. Невозможно спланировать атаку, не собрав предварительно все необходимые данные.

Илл. 9.1. Стадии СИ

После проведения сбора данных из открытых источников вы узнаете, как в компании используются социальные сети и другие средства коммуникации, где расположены офисы. В вашем распоряжении будут и другие подробности внутренних корпоративных механизмов — а значит, вам будет намного проще разработать подходящую и эффективную легенду.

Дальше логично перейти к планированию векторов атаки. Будете ли вы устраивать фишинговую рассылку? Или собирать личную информацию с помощью вишинга? Может, нужно будет использовать мобильные устройства? Придется ли пробираться на территорию компании? А может, стоит использовать сразу несколько векторов? Все эти вопросы помогут составить полноценный план атаки.

После составления плана можно будет переходить к его реализации: сбору данных на всех этапах атаки и подготовке отчета о проделанной

работе. На практике, однако, нередко оказывается, что провести пентест в строгом соответствии с этими шагами не удается. Скажем, вы завершили сбор данных из открытых источников, на основании которого выбрали отличный вектор атаки, но затем выяснилось, что без сбора дополнительной информации не обойтись — в таком случае логично вернуться к первому шагу.

Вне зависимости от того, какую последовательность шагов необходимо будет осуществить для проведения конкретной операции, в процессе пентестинга всегда должны учитываться следующие принципы:

- Необходимо заранее понимать, собираетесь ли вы записывать телефонные разговоры. Во многих штатах запись разговоров без согласия собеседника считается нарушением закона. Не стоит полагать, что, наняв вас, клиент автоматически дал согласие на любые действия с вашей стороны. То же самое касается записи видео в процессе проникновения на территорию объекта. Обязательно давайте клиенту подписывать официальное согласие на подобные действия.
- Не думайте, что клиент представляет себе все необходимые для проведения социально-инженерного пентеста шаги. Проговаривайте все услуги, которые готовы предложить, чтобы заказчик ясно представил себе, чего ожидать. Такое обсуждение позволит ему задать вам всевозможные вопросы, ответив на которые вы сможете свободно и не создавая ни для кого проблем двигаться дальше.
- Обязательно расписывайте все шаги поиска через Google и называйте инструменты, которые используете в ходе подготовки. При желании клиент должен иметь возможность повторить ваши действия.
- Некоторые пентестеры переживают, что тем самым лишат себя работы: якобы после этого клиент сможет проводить проверки самостоятельно. Но за годы работы я ни разу не потерял заказчика из-за того, что слишком многому его научил.
- Процесс так же важен, как и результат.

  Да, вы можете сообщить клиенту, что 90% получателей перешли по ссылке из письма, а 47% сотрудников, которым вы звонили, сообщили свои идентификационные данные по телефону. Получится пугающая статистика, но ведь это еще не все. Вы должны объяснить заказчику каждый проделанный в процессе подготовки шаг, мотивировать выбор конкретного вектора атаки, а также выделить людей, которые не повелись на ваши уловки, — потому что все это не менее важно, чем цифры и проценты.

- Не стоит активно публиковать в социальных сетях информацию об эксплойтах, которые сработали на ваших клиентах. (Очень

неприятно бывает сталкиваться со специалистами, которые это практикуют.)

- Представьте, что вы обратились к врачу за весьма неприятной процедурой, в ходе которой он побывал в таких закоулках вашего тела, куда никому не стоит соваться. Этот опыт был для вас крайне неприятным, возможно даже болезненным, и уж точно заставил вас покраснеть. Но процедура наконец завершена, и врач на минуту отлучился из кабинета. Ожидая его возвращения, вы достали телефон, чтобы глянуть, не написал ли кто чего-то важного в соцсетях. Как вдруг увидели свежий твит своего врача: «Зацените размер опухоли, которую я только что нашел у одного жирного недотепы. Ахах». Да, имени вашего он не называл и лица вашего никто не увидит, но тем не менее, что вы почувствовали бы? Понравился бы вам такой доктор? Поверили бы вы, что он желает вам добра? Я бы точно не вернулся к такому врачу.

  То же самое касается постов о том, как легко вам удалось проникнуть в офис клиента или как плохо у него организована охрана. Такие публикации заставляют людей ощущать стыд. Делать их просто непрофессионально.

На эти пять принципов можно ориентироваться при подготовке любой операции. И прежде чем переходить к правилам организации каждого из векторов атаки, хочу дать вам еще два совета: документируйте все и придирчиво выбирайте легенды.

Зачем все документировать

Клиенты платят вам за максимально тщательное исследование вопросов безопасности их компаний. Поэтому даже если какой-то материал, найденный в открытых источниках, для организации атаки не пригодился, сообщить о его существовании заказчику все же стоит. Безусловно, иногда вы будете находить информацию, которая сможет нанести заказчику серьезный вред. Как поступать в таком случае?

Однажды нашей компании заказали проверку того, насколько одна высокопоставленная руководительница финансовой компании соблюдает необходимые требования безопасности. В процессе поиска мы обнаружили фотоснимки, которые она делала в молодости и которые из промоматериалов фотографа перекочевали на порносайт. Что делать в такой ситуации социальному инженеру?

Мы решили, что такая информация слишком деструктивна, чтобы использовать ее в фишинге. Поэтому для пентеста мы выбрали другую стратегию. Но уже после завершения проверки запросили личную встречу с этой руководительницей, рассказали ей о своей находке и предложили помощь в том, чтобы добиться удаления фотографий с

сайта без огласки в компании. Женщина была очень нам благодарна, и я до сих пор поддерживаю с ней дружеские отношения.

Зачем выбирать легенды придирчиво

Я бесчисленное количество раз находил информацию, порочащую клиентов, но сознательно ни разу не использовал ее при составлении легенд. Возможно, некоторые читатели подумают, что из-за этого я упускаю многообещающие возможности. Однако я всегда руководствуюсь правилом, которое уже не раз упоминал и сейчас с удовольствием повторю снова: после встречи со мной люди должны чувствовать себя лучше, чем до нее. Кроме того, я стремлюсь к тому, чтобы проверка служила в первую очередь обучающим целям — а человека, который чувствует себя униженным, сложно чему-то научить. Следовательно, к легендам я отношусь крайне придирчиво и тщательно выбираю, какую информацию использовать, а какую — нет. И да, я советую документировать все, что попадется вам на глаза в процессе подготовки. Таким образом, даже если вы не используете эту информацию в легенде, вы должны сообщить ее клиенту.

Один клиент как-то заказал у нас фишинг. Выяснилось, что один из его сотрудников использовал корпоративную почту при регистрации на сайте для «особых» знакомств. Там этот человек публиковал комментарии под фото весьма привлекательных обнаженных женщин: писал, что приезжает в их город в командировку и хотел бы встретиться. Сейчас я предлагаю вам отвлечься от моральных суждений о его изменах жене или компрометирования корпоративной почты на подобном сайте. Поразмышляйте о ситуации с другой точки зрения: сработал бы фишинг от одной из таких дам с сайта? Я почти со 100%-ной вероятностью могу гарантировать: да, сработал бы. Но мы такой заход использовать не стали. Ведь цель профессионального социального инженера — просвещение и помощь, а не унижение.

Фишинг

Фишингом называется отправка зараженных электронных писем из якобы проверенных источников. Цели фишинга могут быть следующими:

- чтобы человек установил на компьютер программы, предоставляющие мошенникам удаленный доступ к системе;
- чтобы собрать личные данные;
- чтобы получить другую информацию, необходимую для проведения атаки.

Содержание, легенда и метод доставки фишингового сообщения определяются его целью. Профессиональные социальные инженеры используют в своей работе несколько типов фишинговых методов.

Образовательный фишинг

Иногда клиентам не требуется, чтобы пентестер проверял технические ресурсы Сети: их интересует исключительно человеческий фактор. Эффективным способом решения такой задачи является образовательный фишинг: после перехода по размещенной в письме ссылке никаких вредоносных кодов или программ для получения удаленного доступа на компьютер объекта не устанавливается. Данный вид фишинга проводится исключительно для сбора статистики и оценки общей уязвимости сотрудников к такому вектору атаки. А еще для определения сфер, в которых необходимо дополнительное информирование.

Чаще всего такой фишинг пробуждает у объекта воздействия любознательность, жадность, радость или здоровый страх, которые и заставляют перейти по ссылке. В таком случае легенда основывается на проведении сбора данных из открытых источников по отдельным сотрудникам или компании в целом. Моей команде приходилось отправлять подобные фишинговые письма как в единственном экземпляре, так и сотням и даже тысячам людей за раз.

Приведу пример, иллюстрирующий необходимость следования принципам, описанным в предыдущем разделе. Я составил для клиента письмо, похожее на реальное приглашение с LinkedIn. Разослал его 7000 пользователей, работавших на него, и быстро получил 73% переходов по ссылке. Такой молниеносный успех вдохновил всех, включая меня самого.

На носу был следующий пентест, и я, недолго думая, решил снова использовать свою гениальную идею. Уже на следующей неделе аналогичный e-mail разлетелся по 10 000 пользователей, работавших на другого заказчика. Но по ссылке перешли всего 4% получателей. Я не мог в это поверить: был использован гениальный заход. Я попросил клиента узнать у сотрудников, в чем заключалась причина провала этого фишинга.

Оказалось, что я сам был виноват. Первая компания занималась производством, большинству ее сотрудников было от 35 до 55 лет. А вторая компания занималась продажами, и возраст ее сотрудников составлял 19–29 лет. Когда последних спросили, почему они не перешли по указанной в письме ссылке, все как один отвечали: «Ну да, я видел это письмо, но LinkedIn используют только старики. Я все вопросы решаю в Facebook».

<рукалицо> Успех первой атаки пьянил меня, и я забыл, что универсальных методов не бывает: каждый раз нужно составлять фишинговые письма, исходя из особенностей компании-заказчика. Этот опыт только укрепил мою уверенность в бесполезности фишинговых

SaaS-сервисов, работающих целиком и полностью за счет готовых шаблонов.

Даже если цель фишинга образовательная, готовить его все равно нужно в соответствии с шагами, описанными на илл. 9.1. Начинать со сбора данных из открытых источников, а затем составлять текст, который придется по вкусу целевой аудитории и позволит достичь поставленной цели.

Фишинг с целью тестирования на проникновение

Этот вид фишинга не отличается от образовательного ничем, кроме самого главного — конечной цели. В данном случае задачей пентестера является получение удаленного доступа, сбор личных данных или любой другой подрыв информационной безопасности компании.

Обычно в контексте этого фишинга у объекта воздействия имеет смысл вызывать такие сильные эмоции, как страх, жадность, удивление или даже печаль. Ведь мне будет недостаточно простого перехода по ссылке: мне нужно, чтобы человек открыл приложенный документ, не задумываясь ответил на сомнительный запрос или ввел личные данные. И поскольку выполнение этих действий требует от человека времени и энергии, эмоциональные триггеры должны быть сильнее.

Например, однажды мне довелось проводить пентест в организации, сотрудники которой в большинстве своем питали горячую любовь к продуктам компании Apple. Почти у каждого был MacBook, а темой общего обсуждения часто становились последние модели iPhone. Пентест совпал со временем выхода одной из них. Поэтому к фишинговому e-mail, который я разослал сотрудникам компании, была приложена фотография нового iPhone. А содержание письма (якобы отправленного из отдела кадров) было следующим:

[Название компании] подарит 10 счастливчикам новый iPhone с оплаченным на год вперед тарифным планом. Розыгрыш смартфонов состоится в следующую пятницу в 15:00. Чтобы принять участие в розыгрыше, перейдите на указанную страницу внутрикорпоративной сети и введите свой рабочий логин и пароль. После этого вы будете автоматические занесены в базу участников https://iphone.updates-company.com.

Удачи!

Мы выкупили домен updates-company.com и создали страницу с логотипом компании, двумя полями для ввода данных и одной кнопкой. Разослали письмо 1000 человек и получили учетные данные от 750 сотрудников.

Вывод: верно подобранный эмоциональный триггер, использованный в правильное время и на правильных людях, — залог успеха любой операции.

Адресный фишинг

Адресный фишинг во всех его вариациях — это самая персонализированная форма фишинга. После проведения сбора данных из открытых источников по объекту воздействия и всем членам его семьи, которых мне удается найти, я обычно выбираю какую-то очень личную информацию и выстраиваю на ее основе легенды. Часто нужную информацию я нахожу в социальных сетях родственников объекта.

Однажды я обнаружил, что группа друзей интересующего меня человека отправилась на мальчишник в Лас-Вегас. Они публиковали столько фотографий своих безбашенных приключений, что я решил использовать это в легенде.

Фишинговый e-mail был написан от лица менеджера отеля, в котором они остановились. Содержание его было следующим:

Мистер [имя],

3–8 июля вы останавливались в нашем отеле. В ходе уборки номера горничная обнаружила предмет, вероятно, оставленный вами. Пожалуйста, взгляните на приложенный снимок и сообщите, ваша ли это вещь.

Если вы ее оставили, перейдите по приведенной ниже ссылке и внесите в форму данные, которые позволят нам оправить вам утерянное имущество.

С уважением,

[Сотрудник отеля]

Зачем я вставил в письмо ссылку, хотя зараженным был приложенный файл и никакой фотографии получатель все равно бы не увидел? Потому что был шанс, что человек, получивший такое письмо, в любом случае признал бы вещь своей. На такой случай в форму предлагалось занести:

полное имя;

почтовый адрес;

номер телефона;

адрес электронной почты;

дату рождения (как доказательство совершеннолетия);

последние четыре цифры номера кредитной карты, которая использовалась для оформления брони номера.

Легенда сработала очень эффективно, потому что человек не только открыл зараженный файл, но и предоставил мне дополнительную информацию для планирования дальнейших атак.

Даже когда я использую в легендировании для адресного фишинга личные данные, то не работаю с информацией, которая может навредить объекту воздействия. Например, в описанном случае я бы не стал использовать легенды вроде: «В нашем распоряжении оказались ваши фотоснимки в компании проституток. Чтобы выкупить эти фотографии, перейдите по ссылке» — даже если такие фотографии действительно существовали бы. И если бы я нашел подобные фотографии в процессе сбора данных из открытых источников, то сообщил бы о них объекту воздействия напрямую и спросил, как он сам хочет разобраться с возникшей ситуацией.

Фишинг: резюме

Не знаю, как вы, а лично я получаю на свои аккаунты в среднем 200–250 электронных писем в день. И как ни странно, проверка e-mail при этом не является моей основной работой!

ТОЛЬКО ЗАДУМАЙТЕСЬ

Согласно отчету компании Radicati Group (http://www.radicati.com/wp/wp-content/uploads/2014/01/Email-Statistics-Report-2014-2018-Executive-Summary.pdf) в 2017 году каждый день отправлялось порядка 269 млрд e-mail. Это 3,1 млн в секунду! И еще один забавный факт: кажется, половина из них прилетает ко мне в папку «Входящие» (ну ладно, может, я слегка преувеличиваю).

E-mail используются для коммуникации между людьми, для бизнеса, шопинга и многих других целей. Поэтому в большинстве СИ-атак используется именно этот вектор. Профессиональный социальный инженер обязан уметь составлять убедительные электронные письма, основываясь на собранных из открытых источников данных. Это единственный способ проверить уязвимость клиентов по отношению к данному вектору атаки.

Вишинг

В 2015 году термин «вишинг» попал в Оксфордский словарь английского языка. Я связывал популярность этого слова с собственной просветительской деятельностью, но никто не верил. (Но в каждой шутке, как известно, есть доля правды.)

Вишинг — это фишинг с использованием голоса. Сегодня этот вектор атаки намного популярнее, чем несколько лет назад. На мой взгляд, рост популярности метода связан с его эффективностью.

Вот несколько причин, по которым стоит использовать вишинг в пентесте:

- сбор идентификационных данных;

- сбор данных из открытых источников;
- непосредственно атака.

Давайте обсудим каждый из них, чтобы вы понимали, чем отличается вишинг, используемый для достижения каждой из этих целей.

Сбор идентификационных данных

Конечно, в процессе пентестинга мы с командой используем технические решения, позволяющие компрометировать безопасность компании. Однако вишинг и фишинг для сбора идентификационных данных мы тоже используем, чтобы упростить процесс.

В ходе одной проверки после проведения сбора данных из открытых источников я собрал 10–15 телефонных номеров и собирался звонить по ним в надежде собрать идентификационные данные. Легенду я сформулировал в соответствии с результатами сбора данных из открытых источников: узнал, что недавно в офисах компании перешли с одной операционной системы на другую и этот переход курировал сторонний IT-подрядчик. Изменилось многое: обновить пришлось не только операционную систему, но и программы, которые часто использовались в работе.

Согласно легенде, я представился Полом из компании «Безопасные IT» (конечно, это название выдумано исключительно для книги). Якобы мне нужно было проверить статус обновлений на компьютере конкретного сотрудника, потому что мы зарегистрировали проблемы на некоторых устройствах. Между нами состоялся следующий диалог:

Объект: Добрый день, Стив слушает. Чем я могу помочь?

Я: Здравствуйте, Стив. Это Пол из компании «Безопасные IT». Я хотел бы…

Объект [перебивает меня]: Так это вы! Знаете, сколько на меня свалилось работы? А ваши чертовы обновления не дают мне ничего нормально сделать!

Я: Я понимаю, Стив. Потому и звоню. Мы заметили подозрительную активность с вашего IP-адреса, и я полагаю, что проблема может заключаться в отравлении DNS в связи с переполнением стека. [В конце этой фразы у меня даже голос дрогнул, а про себя я молился, чтобы Стив не оказался айтишником.]

Объект: Мой компьютер отравлен? Что вы вообще такое говорите, Пол?!

Я: Извините, это профессиональный жаргон. Правда, простите. Я хотел сказать, что в процессе установки могли возникнуть проблемы, из-за которых теперь компьютер работает медленно. Могу ли я сейчас попросить вас выполнить несколько действий, которые позволят устранить неполадки?

Объект: Послушайте, Пол. Пришлите сюда представителя, чтобы он сделал все что нужно. Я вообще не понимаю, что вы мне тут говорите на своем жаргоне.

Я: Ничего страшного, Стив. Но направить к вам сотрудника удастся не раньше, чем через четыре-пять дней. Но я могу помочь вам удаленно, прямо сейчас. Для этого мне нужно только залогиниться и установить удаленный доступ к вашему компьютеру.

Объект: Если это решит проблему — я обеими руками за. Что мне нужно сделать?

Я: Я могу залогиниться прямо сейчас и внести все необходимые поправки. Для этого мне нужны только ваш логин и пароль, которые вы используете для входа.

Объект [ни секунды не колеблясь]: Логин SMaker, S и M большие. Пароль у меня хороший, так что не крадите: Krikie99.

Вот так просто в моих руках оказались ключи от рая.

В процессе сбора идентификационных данных мне очень помогают открытые источники, помогающие придумывать максимально правдоподобную легенду с использованием актуальных или важных для объекта воздействия деталей. С помощью вишинга мне удавалось получать идентификационные данные для входа в домен, VPN, электронную почту, защищенные базы данных и даже коды от входных дверей.

Вишинг в сборе данных из открытых источников

Иногда собрать необходимые данные в открытых источниках не удается, или же до проведения атаки возникает необходимость проверить собранную информацию. Однажды мне понадобилось провести адресный фишинг и вишинг по одному человеку, но было непонятно, какой именно почтовый ящик и телефонный номер использовать: мы нашли сразу несколько.

Поэтому мы придумали легенду для определения его актуального адреса и телефона. Мы узнали, что объект часто летал из Канады в Лондон. Уточнили номер лондонского отеля Hilton и обзвонили «с него» все предполагаемые номера объекта с помощью спуфинга (так называется форма атаки, в процессе которой абоненту передаются ложные идентификаторы звонящего. — Прим. пер.).

Объект: Алло?

Я: Добрый день. Это мистер Альфред Гейнс?

Объект: Да, это я. Кто спрашивает?

Я: Прошу прощения, меня зовут Пол, я звоню из отеля Hilton в Лондоне. Могли бы вы выделить минуту своего времени и оценить ваш последний

опыт пребывания в нашем отеле? Для этого нужно ответить на несколько вопросов, это займет не больше полминуты…

Объект: Опыт пребывания? Вы о чем? Я не был в Лондоне уже несколько месяцев. Откуда у вас этот номер?

Я: Прошу прощения за доставленные неудобства. Еще раз уточню: вы — Альфред Гейнс и ваш номер 846-555-1212, верно?

Объект: Все верно, но, скорее всего, у вас ошибочная информация о том, когда я у вас останавливался.

Я: Понимаю. Скажите, а могу ли я отправить вам чек, чтобы вы могли подтвердить, ваш он или нет?

Объект: Да, конечно.

Я: Большое спасибо. Уточните, пожалуйста, адрес вашей электронной почты? A.gaines@hmail.com?

Объект: Лучше отправьте на gainesat@gmail.com, его я проверяю намного чаще.

Я: Еще раз большое спасибо, сэр. Сейчас же вышлю.

Таким образом мы подтвердили актуальный номер телефона и электронный адрес объекта, а также нашли вектор атаки, позволивший нам получить всю необходимую информацию.

Мы с командой часто используем эту технику для подтверждения и дополнения уже собранных данных. Я считаю эту форму вишинга особенно эффективной, потому что она не дает объекту времени на раздумья. Более того, многие компании не информируют сотрудников о возможности подобного мошенничества. А зря. Они очень рискуют.

Вишинг в процессе атаки

Самого по себе вишинга бывает достаточно, чтобы скомпрометировать безопасность компании. Принципы при этом сохраняются те же: правильно подобранная легенда и убедительные доказательства ее истинности позволяют социальным инженерам вытягивать у людей даже самую опасную информацию.

Однажды перед нашей командой была поставлена задача с помощью вишинга проверить безопасность крупной финансовой компании. Изображая руководительницу высшего звена, мы должны были проверить, удастся ли через рядовых сотрудников компании получить ее логин и пароль, а также любую другую информацию о системах и данных, которыми она пользуется.

В качестве легенды мы решили использовать образ руководительницы, которая улетала на Гавайи, где собиралась провести медовый месяц. Но ей якобы позвонил начальник и сказал, что не может найти отчет — а он просто необходим на встрече, которая состоится уже в понедельник.

Женщина знала, что отчет хранится на рабочем столе ее компьютера, но забыла имя пользователя, с помощью которого можно было бы получить удаленный доступ.

Мы нашли на YouTube трек под названием «звуки аэропорта» и набрали номер службы поддержки (я сидел рядом с сотрудницей, которая изображала ту самую руководительницу, слушал разговор и был готов подсказывать по мере надобности).

Объект: Служба поддержки. Чем я могу вам помочь?

СИ-агент [громко вздохнула и сказала напряженным голосом]: Меня слышно? В аэропорту очень шумно.

Объект: Да, я вас слышу несмотря на шум. С кем имею честь общаться?

СИ-агент: О, прошу прощения. [Снова вздыхает.] Это Дженнифер Тилли, исполнительный финансовый директор. Я улетаю на Гавайи на медовый месяц, и только что мне позвонил мой начальник и сказал, что последний отчет по бюджету до него не дошел. Этот отчет необходим ему для встречи в понедельник. Мне нужно залогиниться и переслать его ему, но я забыла логин.

Объект: Понял. Сейчас посмотрим, как вам помочь. Мне необходимо будет подтвердить вашу личность. Но прежде позвольте поздравить вас со свадьбой и пожелать отличного отдыха на Гавайях.

СИ-агент: Большое спасибо. Я жду с нетерпением, потому что раньше там не была, а теперь наконец побываю со своим лучшим другом и по совместительству мужем.

Объект: Еще раз поздравляю. Очень радостно слышать, когда люди счастливы. Ну что ж, миссис Тилли, назовите, пожалуйста, ваш идентификационный номер.

СИ-агент: Знаете, я обещала мужу эти две недели к работе даже не притрагиваться, поэтому у меня с собой нет ни ноутбуков, ни ID. Я даже свою дату рождения иногда забываю, что уж говорить про идентификационный номер.

Объект [стараясь быть максимально услужливым]: Хотя бы попробуйте. Я вам подскажу: первые цифры 1 и 7. Осталось вспомнить всего 5 цифр. [Эта информация оказалась в дальнейшем крайне полезной.]

СИ-агент: Вообще не помню. Эээ, может 98231?

Объект: Да, в номере есть 9 и 8, но номер не правильный. Давайте попробуем иначе. Можете назвать имя своего руководителя?

СИ-агент: Конечно. Майк Фарели.

Объект: Отлично. А адрес электронной почты?

СИ-агент: j.tilly@companyname.com.

Объект: Все верно. Что я могу сделать, хм… Я могу ввести новый пароль и отправить его на ваш телефон, после чего вам останется только войти в свой аккаунт и отправить необходимый документ. Секундочку… [послышалось, как он что-то печатает]. Простите, миссис Тилли, но на ваше устройство, оказывается, до сих пор не установлено ПО для получения удаленного доступа. Так что даже если я поменяю для вас пароль, вы не сможете войти.

СИ-агент: Только не это. Это же просто ужасно. Меня не будет две недели, посадка начинается через полчаса. Что же делать?! Пожалуйста, помогите мне решить эту проблему! [Со слезами в голосе.]

В это время я написал коллеге записку, в которой предлагал намекнуть объекту воздействия, что он может установить программу для получения удаленного доступа на компьютер руководительницы и сообщить ей пароль для одноразового использования.

Объект: Можно отправить запрос на установку ПО для удаленного доступа, однако это займет несколько часов — и то в лучшем случае. Скорее всего, это не будет сделано до завтра.

СИ-агент: Спасибо вам огромное за помощь. Муж так злится: мы должны были пить шампанское и ждать посадки, а я опять ушла и никак не могут отвлечься от работы. Пожалуйста, скажите, можно ли каким-то образом сделать это быстрее?

Объект: Не переживайте, миссис Дженнифер, вы прекрасно проведете свой медовый месяц. Сейчас мы что-нибудь придумаем. Повисите несколько минут на линии.

СИ-агент: Хорошо, только, пожалуйста, не слишком долго. У нас вот-вот начнется посадка.

После мы услышали, как объект сказал коллеге: «Бедная женщина уже в аэропорту, улетает на медовый месяц и не может получить доступ к своему компьютеру, чтобы срочно решить одну проблему. Мы же можем как-то ей помочь?»

Конкретного содержания ответа мы не расслышали, но по тону догадались, что Дженнифер, по-видимому, будут пытаться спасти всем отделом. Через несколько минут объект поставил звонок в режим ожидания, но вскоре вернулся к разговору.

Объект: Миссис Тилли, у нас для вас есть свадебный подарок. Мой коллега прямо сейчас устанавливает на ваш компьютер нужную программу. Где-то через 10 минут вы сможете получить необходимый документ.

СИ-агент: Огромное вам спасибо, вы не представляете, как я вам благодарна! И мой муж будет просто счастлив, лучшего подарка и не придумаешь! Спасибо!

Объект: Как только коллега сообщит мне, что программа установлена, я отправлю вам на телефон одноразовый пароль. И вы сможете отправить необходимый документ.

СИ-агент: Ой, подождите, так не получится… Я же не взяла с собой рабочий телефон, я не смогу получить СМС…

Объект: Но, миссис Тилли… это правило обойти нельзя. Я не знаю, что еще можно сделать.

СИ-агент: Как же это ужасно. Это мне урок на всю жизнь!!! Как можно быть такой тупицей! Нужно всегда носить с собой рабочий телефон, всегда! Получается, придется отменять перелет и откладывать отпуск. Все равно огромное вам спасибо за помощь, что поделаешь, если я такая дура…

Объект: Нет! Нельзя так поступать, у вас же медовый месяц… [шепотом]: Послушайте, давайте я отправлю вам код в СМС на рабочий номер, а после просто зачитаю его вслух?

СИ-агент: Вы готовы это сделать? Боже мой, я сейчас заплачу.

Объект: Нет, не стоит. Сейчас мы все сделаем, и вы спокойно сядете на свой рейс и полетите отдыхать, не думая о работе.

Таким образом нам удалось получить удаленный доступ, пароль — и найти возможность серьезно навредить компании.

СОВЕТ ПРОФИ Наверное, вы заметили, что я люблю эмоциональные легенды, в которых объект воздействия «помогает» или даже «спасает» меня. И не безосновательно. Когда мы даем человеку возможность довериться нам, в свою очередь доверяясь ему, это создает между нами сильную связь. Выделяется окситоцин, заставляющий человека быть последовательным в своем желании помочь вам, вне зависимости от того, насколько это действие может оказаться небезопасным.

Использование вишинга в качестве основной стратегии атаки может значительно облегчить работу пентестера. А убедительная легенда для успешного телефонного разговора основывается на открытых данных, которые, в свою очередь, можно собрать с использованием того же вишинга.

Вишинг: резюме

Вишинг — эффективный вектор атаки. С его помощью злоумышленники могут нанести компании существенный урон. Он может использоваться на разных этапах социально-инженерной атаки, и потому считается одним из самых мощных инструментов в СИ-арсенале.

Профессиональный социальный инженер, желающий достичь в своем деле успеха, не должен бояться телефонных разговоров. Учитесь их вести, даже если в обычной жизни предпочитаете общаться лично.

Нужно уметь устанавливать раппорт, заручаться доверием и получать информацию от объектов воздействия, даже когда они вас не видят.

SMiSHing

Раздел, посвященный этому методу, будет довольно коротким, потому что специалистам по проверке безопасности редко приходится использовать СМС-сообщения в ходе атаки. После скандала с Wells Fargo в 2017 году прокатилась волна СМС-мошенничеств. Многие из них были выстроены по той же схеме, что и текст на скриншоте 9.2. Большинство таких сообщений сформулированы просто, однако весьма эффективно справляются со своей задачей (которая чаще всего заключается в загрузке вредоносного кода на мобильное устройство и последующей кражи персональных данных).

Перевод: Важное сообщение от отдела безопасности.
Зарегистрируйтесь, чтобы прочесть -=>

Илл. 9.2. Популярный вид СМС-мошенничества после скандала с Wells Fargo в 2017 году

В последние годы все чаще организуются атаки с использованием вредоносных кодов для мобильных операционных систем, направленных на получение доступа к устройству жертвы. Кроме того, все шире распространяется практика использования сотрудниками личных устройств на работе (BYOD). А взломав мобильное устройство, злоумышленники получают возможность читать электронную почту его владельца, удаленно включать видеокамеру и микрофон, а также использовать его как удаленную точку доступа. Разумеется, это вызывает беспокойство у представителей многих организаций.

Именно поэтому социальные инженеры тоже должны владеть этим методом воздействия. Вот несколько правил, отличающих SMiSHing от фишинга:

Краткость всему голова. Сообщение должно быть коротким и понятным. Никаких вступлений и заключений — только факты и ссылка.

Ссылки. Я считаю, что всегда имеет смысл создавать под атаку соответствующее доменное имя. Однако если сделать это невозможно,

укороченные URL намного лучше работают в СМС, чем в электронной почте. Проверить ссылку на мобильном устройстве намного сложнее, поэтому только продвинутые пользователи сумеют заподозрить, что со ссылкой что-то не так.

Не скупитесь. Если ваша задача — сбор личных данных, не рассчитывайте, что объект воздействия не обратит внимания на неправдоподобность внешнего вида созданной вами страницы. Поэтому, чтобы СМС-проверка выявила все возможные угрозы, потратьте время на создание правдоподобных веб-страниц.

Не усложняйте. Объекты воздействия используют мобильные устройства, а значит, чем больше шагов им нужно будет сделать, тем ниже вероятность, что они пройдут этот путь до конца.

Чем больше сотрудников используют на работе собственные устройства (или вообще работают из дома), тем актуальнее становится этот вектор атаки для социальных инженеров.

В ближайшем будущем мобильные телефоны никуда не исчезнут. Более того, с годами их многофункциональность только увеличится, они все плотнее вписываются в нашу профессиональную жизнь. А значит, отслеживать подобные атаки будет еще сложнее.

Имперсонация

Имперсонация (выдавание себя за другого человека) — один из самых опасных для компаний и один из самых рискованных для социальных инженеров видов атаки. Поэтому его используют реже всего. Имперсонация предполагает, что социальный инженер изображает сотрудника компании-объекта или вызывающее доверие и обладающее определенными полномочиями лицо (представителя правоохранительных органов, наемного работника и т.п.).

Мы с моей командой получаем огромное удовольствие от подобных заданий, но, справедливости ради, надо учесть, что при этом мы практически ничем не рискуем. Если же на имперсонацию пойдет злоумышленник, ему придется планировать атаку тщательнейшим образом. У пентестеров есть возможность заручиться письмом, «освобождающим от тюрьмы»: оно позволит избежать проблем с законом даже в случае неудачи. Понятное дело, плохие парни этой привилегией не пользуются.

ИМПЕРСОНАЦИЯ И РЕДТИМИНГ

Редтиминг обычно (хотя и необязательно) проводят ночью. Обычно цель таких операций — преодоление физических систем безопасности: проникновение в лифты, взлом замков, обход камер наблюдения и т.п. А социальные инженеры, использующие имперсонацию, в первую очередь изучают человеческий фактор в обеспечении безопасности здания.

Поэтому мы не взламываем замки, а работаем с человеком, у которого хранится ключ или пропуск — чтобы он сам распахнул перед нами нужную дверь. Одним словом, специалисты по редтимингу сосредоточены на технологиях, а социальные инженеры — на людях.

Планирование имперсонации

В процессе пентеста социальный инженер должен помнить, что имперсонация предполагает взаимодействие со всеми органами чувств объекта. То есть если во время фишинга мы работаем только со зрением, а в вишинге — со слухом, то, перевоплощаясь в другого человека, нам приходится взаимодействовать со всеми органами чувств объекта (за исключением, пожалуй, вкусовых рецепторов).

Поэтому крайне важно планировать подобные проверки в соответствии с описанными ниже принципами и шагами.

Сбор информации

Сбор информации — важная часть подготовки к заданию. Я часто прошу посетителей моих курсов назвать легенду, которая гарантирует получение доступа в помещение. Подумайте и вы, что бы это могло быть?

Многие предлагают изображать курьера службы доставки вроде UPS. Но вопросы, которые я задаю, заставляют их пересмотреть свое решение: «Отлично, а что потом? Вы часто видите представителей UPS, шныряющих по коридорам без присмотра? Обычно их перемещения по зданию заканчиваются в приемной или в канцелярии».

Сбор данных из открытых источников — основа создания правдоподобной легенды для имперсонации. В ходе одной операции я обнаружил, что из-за строительных работ, проводившихся неподалеку от интересовавшего меня здания, пауки вышли из зимней спячки раньше обычного. Жителей района это беспокоило: проблему даже освещали в местных новостях. Поэтому я выбрал легенду специалиста по борьбе с пауками. Сработало на ура.

Разработка легенды

Мы уже говорили о разработке легенды, когда обсуждали процесс сбора информации. Но поймите меня правильно: нельзя планировать легенду до проведения сбора данных из открытых источников. Кроме того, после выбора легенды нужно внимательно обдумать все детали: одежду, необходимые инструменты, внешний вид и т.п. Иногда бывает необходимо заранее привести одежду в состояние «бывшей в употреблении». Не упустите детали, которые добавят правдоподобности вашей легенде. Лучше перестраховаться.

Недавно мне с коллегой нужно было найти способ пробраться в несколько офисов одного банка. С помощью открытых источников я узнал, что этот банк только что прошел проверку на соответствие стандартам безопасности данных индустрии платежных карт (PCI compliance test). Мы узнали название проводившей ее компании, подделали их униформу, бейджи и визитки, благодаря чему без проблем прошли в центр проверки банкоматов. Там мы сумели получить доступ к двум компьютерам и даже к идентификационным данным других сотрудников, работавших по соседству.

Но, когда к нам подошел менеджер и попросил назвать наше контактное лицо из компании, мы растерялись. Я заранее об этом не подумал, и из-за такой вот мелочи нас поймали с поличным. Тем не менее к тому моменту мы уже почти полчаса провели в центре проверки банкоматов с неограниченным доступом к нескольким компьютерам и успели проникнуть в Сеть. Но если бы мы продумали и ту деталь, она могла бы обеспечить нам больше времени на территории и повлиять на исход операции.

Планирование и реализация атаки

Определившись с легендой, подробно сформулируйте, что вам нужно будет сделать после проникновения в здание. А также чего вам категорически нельзя делать. Можно ли вам устанавливать удаленное подключение? Подрывать работу сервера? Разрешено ли уносить из офиса какие-либо устройства? Не думайте, что факт вашей связи с заказчиком позволяет вам в роли «плохого парня» делать все что заблагорассудится. Такое заблуждение может дорого вам обойтись.

Поэтому ваша задача — спланировать атаку от начала и до конца, а затем убедиться, что у вас на руках есть все необходимые и заранее проверенные инструменты для достижения поставленных целей.

Когда же план будет готов, не забудьте получить от заказчика то самое письмо, которое позволит вам не угодить за решетку: в нем должны быть прописаны ваши задачи и полномочия. Старайтесь не упустить ничего.

Идеальная подготовка — залог идеального результата.

Отчет

Самая важная часть любой операции — разъяснение заказчику подробностей проделанной работы и ее результатов. Также необходимо помочь клиенту определиться с направлением дальнейших действий. Прежде чем приступать к атаке, обязательно получите от клиента согласие на аудио- и видеосъемку. Если же вам его не дадут, продумайте, как будете собирать информацию для подготовки отчета.

Я всегда стараюсь представить любую атаку как своего рода историю — чтобы клиент видел, слышал и чувствовал происходящее. Чтобы он

понял, что сработало и почему. Практика показывает: полезно хвалить клиентов за корректные действия сотрудников и быть скромнее в отношении собственных достижений.

Цель составления отчета — та же, что и у любого социально-инженерного взаимодействия: чтобы после прочтения отчета клиент почувствовал себя лучше, чем до него. А значит, мы не можем позволить себе хвалиться, стыдить кого-либо и уж тем более кого-то унижать.

Соблюдение этих принципов поможет выдержать нужное направление в процессе атаки. На мой взгляд, коллеги редко уделяют этому аспекту деятельности достаточно времени. Кроме того, я знаю, как часто возникают вопросы о том, какую именно информацию включать или не включать в отчеты. Ниже я приведу некоторые соображения о том, как поступать в случае получения конфиденциальной информации.

Насколько законно использовать записывающие устройства

Хочу подчеркнуть: я не юрист, так что мои слова не нужно воспринимать как истину в последней инстанции. И уж точно стоит хотя бы раз проконсультироваться в таких вопросах с профильным специалистом.

При работе с клиентами мы в моей компании поступаем следующим образом:

- Еще до того, как приступить к проверке безопасности компании, мы изучаем законы штата и/или страны в отношении аудио- и видеосъемки.
- Получаем письменное согласие на оба типа записи от заказчика.
- Мы НИКОГДА не записываем речь человека без разрешения.
- И, даже получив разрешение, мы впоследствии «обезвреживаем» полученные записи: удаляем все имена, упоминания места работы и любые другие идентифицирующие собеседника слова.
- Обязательно передаем записи клиенту, чтобы тот мог использовать их в образовательных целях.
- Внимательнейшим образом контролируем безопасность хранения, передачи и использования этих записей.

Важно понимать связанные с вашими действиями риски, а также четко продумывать дальнейшее использование собранных данных. В ходе одной операции сотрудница компании, ставшая объектом воздействия в ходе проверки безопасности, ввела свой рабочий ID и пароль в мой компьютер. И поскольку я получил на это разрешение от заказчика, то записал на видео не только ее лицо, но и введенные данные. Однако в последствии, чтобы не ставить ее в неловкое положение перед начальством, изображение ее лица на видео я «размыл». Конечно, клиент имел полное право запросить видео без обработки. Но я решил поступить именно так — и оригиналы видео в итоге никто у меня не

попросил. Ведь в конце концов, такие съемки должны служить образовательной цели, а не заставлять человека снова и снова переживать неприятный для себя момент.

Когда нужно задуматься об обработке видео

В ходе одной проверки я, как обычно, записывал происходящее на камеру, спрятанную в планшете. Старательно избегая столкновения с охраной, пробрался в серверную и вдруг наткнулся на пару, которая занималась… не тем, чем принято заниматься на рабочем месте. (Да, да, сексом, если вы до сих пор не догадались.) Это неожиданное столкновение на секунду выбило меня из роли социального инженера: парочка злобно накричала на меня, и я в смятении выбежал из помещения. Лишь позже я понял, что из-за непрофессионального поведения этих влюбленных в моем распоряжении оказалась почти минутная запись полового акта. Очевидно, такую информацию отправлять клиенту не стоило — так что мне пришлось думать, что теперь с ней делать.

Клиент заплатил мне за проверку безопасности компании, сети и сотрудников немалые деньги, а действо, свидетелем которого я невольно стал, было грубым нарушением политики компании. Причем один из этой парочки мог и вовсе оказаться злоумышленником, использующим соблазнение как метод манипуляции. Значит, я все-таки должен был сообщить руководству об этом инциденте, который потенциально мог привести ко взлому систем.

СОВЕТ ПРОФИ В шпионском мире специалиста, который внедряется в коллектив с целью соблазнения одного из сотрудников и получения от него конфиденциальной информации, называют «медовым горшочком» (honeypot). Такое же прозвище присваивают и системе (компьютеру), которую используют для сбора данных у ничего не подозревающих пользователей.

Итак, решение было принято. В итоге мужчину — участника событий уволили. Почему не его подругу? Оказалось, что она в компании даже не работала: сотрудник просто провел в серверную совершенно постороннюю женщину и предался там с ней забавам, которые уместны дома или в номере отеля — но никак не на рабочем месте.

Только вам решать, какие из добытых записей в итоге удалять, а какие — нет. Обычно я провожу «чистку», когда человек на записи не совершает ничего противозаконного или нарушающего политику компании: он просто попал в социально-инженерную ловушку, не имея при этом злых намерений. Как я уже говорил, целью своей работы я вижу обеспечение безопасности, а не увольнение людей.

Тем не менее если я обнаруживаю сотрудников, которые смотрят на работе порнографию, занимаются сексом, получают

несанкционированный доступ к данным или, не дай бог, каким бы то ни было образом нарушают права детей, рассчитывать на снисхождение с моей стороны им не стоит.

Закупка оборудования

Найти «шпионское оборудование» можно в самых разных местах[17]: от Amazon до специализированных магазинов (один из моих любимых — https://spyassociates.com). Выбирай — не хочу. Нужно помнить, что класс оборудования обычно соответствует его цене. Встроенная в пишущую ручку камера за $25 будет давать пикселизованное и дрожащее изображение, а вот имитирующая пуговицу камера, за $600 с функцией записи на DVR, конечно, выдаст совсем иное качество материала.

Поэтому я рекомендую внимательно изучать отзывы и информацию о товаре перед покупкой. Лично я всегда:

- уточняю условия возврата товара, чтобы не пришлось высылать его в другую страну в случае поломки;
- читаю отзывы как о конкретном продукте, так и о компании-производителе, чтобы не зря тратить деньги.

ОБРАТИТЕ ВНИМАНИЕ Скорее всего, вам придется хорошенько поднапрячься с поиском удачных ракурсов для съемки, прежде чем это станет получаться автоматически. Поэтому для упрощения задачи я рекомендую использовать одновременно несколько камер. Какая-то из них точно снимет то, что надо.

Имперсонация: резюме

Воплощение этого вектора атаки на практике весьма облегчает грамотное планирование. Помните: взломом помещений и прочим редтимингом социальные инженеры не занимаются, а значит, вам надо заранее сформировать представление о системе обеспечения физической безопасности на объекте.

Каждый СИ-пентестер должен четко представлять себе масштаб действий, необходимых для достижения поставленных клиентом целей. Особенно это касается составления раздела отчета, в котором будут описаны способы решения выявленных проблем. Этот раздел будет полезен клиенту лишь в том случае, если вы поймете и опишете не только «что» сработало, но и «почему».

В последнее время все чаще появляются новости о подрывах системы безопасности с использованием зараженных флешек и специальных устройств. Поэтому профессиональный СИ-пентестер просто обязан освоить имперсонацию и предлагать клиентам этот вектор атаки.

Составление отчета

Когда я только начинал свой профессиональный путь социального инженера, мне поступил заказ: протестировать возможность проникновения на семи складах одной компании. Я справился с задачей на 100%. На один из складов я даже пробрался дважды, в один и тот же день, использовав разные легенды.

Успех меня окрылил. Я собрал все записи и приготовился отчитаться перед клиентом. Руководитель проекта сказал, что нужно написать отчет, и выслал шаблон документа, в котором было несколько заголовков.

Мне кажется, я сидел, уставившись на эти пустые страницы, несколько часов. Потом начал составлять отчет: что-то писал, удалял, снова пытался начать. Я корпел над документом несколько дней, а когда закончил, был уверен, что создал настоящее произведение искусства.

Мне так и представлялись восторги клиента: как его команда прочтет отчет, восхитится и, когда я приду к ним в офис, под ноги мне в знак признательности полетят розовые лепестки. В таком вдохновленном настроении я отправил документ заказчику и стал ждать похвалы.

Через день зазвонил телефон, и я услышал примерно следующее (имейте в виду, здесь, в книге, я привожу смягченные формулировки):

«Крис, что за вонючую кучу мусора я от тебя получил? Это шутка какая-то? Ты что, тут самый главный весельчак? Неужели ты всерьез думаешь, что такой отчет кто-то примет? Доведи его до ума сейчас же!»

Отчет, который он мне прислал на доработку, был испещрен разноцветными исправлениями и комментариями. Казалось, ни один абзац не избежал редактуры.

На внесение исправлений у меня ушло две недели. Этот отчет смело можно назвать самым неудачным за всю мою СИ-карьеру. Но в то же время он меня многому научил. Я понял, как должен выглядеть хороший отчет и как его нужно готовить. Первая версия моего «шедевра» была посвящена тому, какой я крутой Джеймс Бонд. Который тем не менее забыл упомянуть целый ряд крайне важных для клиента подробностей.

Мне не хочется превращать эту главу в конспект семинара по подготовке отчетов. Но все же несколько основополагающих принципов я назову.

Профессионализм

Профессионализмом называется умение действовать в соответствии с профессиональными нормами. Возьмем, к примеру, врача: направляясь к нему, вы рассчитываете на его профессионализм. Но только представьте ситуацию: вы входите в кабинет доктора, а он восклицает:

«Матерь божья, чем же питается этот огромный кит?!» Затем он хлопает вас по плечу и улыбаясь заверяет, что это «просто шутка».

Думаю, мало кому понравилось бы такое обращение. Вот и наши клиенты тоже не хотят слышать фразочки типа: «Как я вас обдурил!», «Представляете, он действительно додумался опубликовать эту информацию!» или «Теперь все ваши склады принадлежат нам» (последнюю фразу я, к сожалению, не выдумал, а позаимствовал из горького личного опыта).

Всегда нужно помнить: отчет прочитают многие люди, и больше всего конструктивных изменений произойдет, если при чтении они не будут чувствовать себя пристыженными или униженными. Стиль изложения, подбор выразительных определений и грамотное представление фактов — вот что поможет вам продемонстрировать свой профессионализм.

Правописание и грамматика

Правописание и грамматика — две мои любимые мозоли. Вектор атаки, не аттаки. Раппорт, а не раппорп. Короче, вы понимаете. Всегда нужно найти время на то, чтобы проверить грамотность ваших отчетов. А еще лучше — отдать их на проверку человеку, профессионализму которого доверяете.

Впрочем, ошибки могут оставаться в документах даже после неоднократных проверок. Бывает. Не нужно стремиться к совершенству, но и отсылать совершенно непроверенный текст тоже не стоит — иначе клиент подумает, что вы относитесь к работе спустя рукава.

Все подробности

Некоторые знакомые мне пентестеры предпочитают исключать из отчетов подробности: как именно они организовали сбор данных из открытых источников, какой была цепочка Google-поиска и т.п. Им кажется, что, получив такую информацию, клиент больше не станет обращаться к ним за услугами, потому что все будет знать сам.

На мой взгляд, это просто глупо. Впрочем, то же самое я не раз слышал и о своей книге «Темные воды фишинга», в которой были подробнейшим образом описаны методы и процессы создания фишинговых программ. Но эффект от книги получился прямо противоположным: компании использовали ее для разработки программ информирования сотрудников по вопросам фишинга, а в процессе обращались ко мне за помощью.

Поэтому я уверен: не стоит переживать, что клиенты получат от вас слишком много информации. Большинство заказчиков оценят ваши знания и находки. И наверняка захотят снова обратиться к человеку,

который настолько уверен в себе как в профессионале, что не боится раскрыть свои карты.

В то же время, если вы наткнетесь на информацию, не предназначенную для распространения, имеет смысл обсудить с вашим контактным лицом в компании дальнейшие действия по ее представлению или не-представлению в отчете.

Защита

Описание действий, необходимых для защиты от будущих атак и от выявленных проблем, можно назвать, пожалуй, одной из важнейших частей отчета — хотя о ней говорят незаслуженно редко. Подумайте сами: как вы отнесетесь к ситуации, когда доктор, сообщив об опасной болезни, желает вам удачи и выходит из кабинета со словами: «Увидимся на следующем приеме… надеюсь»? Вот и с клиентами так себя не ведите. Предлагайте им конкретные шаги, которые можно будет предпринять для разрешения выявленных проблем.

Если же вы предложите банальности или чушь, что это даст клиенту? Предположим, в ходе проверки нежелательные действия совершили 80% сотрудников, подвергшихся вишингу. Как думаете, какие рекомендации по минимизации нежелательных последствий окажутся полезнее для клиента?

- 1-й вариант

  Социальный инженер рекомендует продолжать проводить тесты и поощрять правильную реакцию на вишинг.

- 2-й вариант

  По результатам анализа кампании социальный инженер рекомендует в процессе информирования сотрудников сделать упор на следующие аспекты:

  - При использовании одних и тех же легенд женщины-пентестеры добивались большего успеха, чем мужчины. Возможно, стоит подробнее рассказывать сотрудникам о механизмах извлечения информации, действующих независимо от пола звонящего.
  - Когда пентестер называл выдуманное имя, лишь 12% сотрудников попытались его проверить. Еще меньшее количество людей решили не раскрывать информацию после того, как завершить проверку не удалось. Таким образом, очевидно, что необходимо информировать сотрудников о возможных последствиях игнорирования этой меры предосторожности.

> При желании мы можем созвониться и обсудить перспективы воплощения этих рекомендаций по мере продолжения тестирования.

Второй вариант лучше, это очевидно. Но слишком часто заказчики вместо практических рекомендаций получают явно сформулированные «для галочки» идеи, которые невозможно воплотить в реальной жизни (к сожалению, и моя команда этим тоже иногда грешила).

И хотя я работаю в СИ уже много лет, все равно постоянно себе напоминаю, что нужно выкладываться для каждого клиента на 100%. В противном случае есть риск стать слишком самонадеянным.

Следующие шаги

Часто, даже получив представление о конкретных мерах защиты, клиенты задаются вопросом: «И что дальше?» Поэтому в финальной части любого отчета крайне важно прописать вероятные шаги, которые предпримет заказчик. Это поможет ему понять, что делать и чего ожидать в будущем.

Конечно, не нужно просто писать: «Увидимся на следующем пентесте». В данном случае стоит руководствоваться принципами, которые я описывал в предыдущем подразделе. Отвечайте на этот вопрос настолько подробно, чтобы в руках у клиента оказались средства, необходимые для дальнейших изменений.

Со многими клиентами у нас заключены договоры на проведение ежемесячных проектов. Но даже это я не считаю поводом расслабляться. Постоянным клиентам тоже хочется вовремя узнавать, нужно ли что-то менять в программах информирования сотрудников, расширять их или адаптировать.

Планомерное выполнение всех описанных шагов поможет вам писать по-настоящему хорошие отчеты, которые принесут клиентам пользу и удовлетворение.

Вопросы СИ-пентестеру

В завершение этой главы я хочу ответить на те вопросы о социальной инженерии в пентестинге, которые мне чаще всего задают. Конечно, осветить все нюансы у меня не получится, поэтому я остановлюсь лишь на самых актуальных. Надеюсь, информация окажется полезной как для состоявшихся социальных инженеров, так и для тех, кто только ступил на этот путь.

Как найти заказчиков?

Пожалуй, по популярности это вопрос №1. Итак, вы решили, что социальная инженерия — ваш путь. Что делать дальше? Нужно с чего-то начинать, а с чего — непонятно. Часто в социальную инженерию приходят люди, строившие карьеру в других областях. Предположим, на протяжении 10 лет вы развивались в совершенно другой сфере, набирали навыки и опыт, ваша зарплата тоже постепенно росла. Если же вы решите поменять специальность, вам придется увеличивать с условного нуля не только знания, но и зарплату. Поэтому надо быть готовым к тому, чтобы:

- выйти из зоны комфорта;
- начать с малого;
- осваивать неизвестные навыки;
- поначалу получать меньшую зарплату.

Если вы на все это готовы, можете смело начинать карьеру в социальной инженерии. Но (вечно попадаются эти противные но и все портят, да?) не стоит ждать, что компании, уже занявшие свое место на рынке, сами будут выходить с вами на связь и предлагать заказы. Социальных инженеров пока не так много, но вам все равно придется продемонстрировать свои конкурентные преимущества по сравнению с другими кандидатами. А для этого надо приложить усилия.

ОБРАТИТЕ ВНИМАНИЕ Не забывайте, что профессиональные социальные инженеры занимаются не только получением доступа в здания банков или сбором данных с помощью фишинга. Большая часть нашей работы происходит в офисе, и существенная доля времени уходит на составление отчетов. Для профессионала социальная инженерия — это не просто умение находить общий язык с окружающими, быстро соображать или не теряться под давлением обстоятельств. Это серьезная работа.

Подумайте, какая из этих сфер может стать вашей слабой стороной:

- извлечение информации;
- умение убалтывать собеседника;
- высокая скорость мышления;
- умение писать хорошие отчеты;
- профессиональный жаргон.

Нужно учиться видеть свои слабости. Только тогда вы сумеете от них избавиться.

Если будет возможность, перейдите по ссылке https://youtu.be/RGnzf66-a4A и посмотрите мое выступление на конференции DerbyCon7, посвященное этой теме. (Сразу предупреждаю: начинается оно с пранка моего друга Дейва Кеннеди, но потом мы быстро переходим к заявленной теме.)

Как склонить клиентов к применению СИ?

Предположим, вы уже являетесь пентестером и готовы заняться социальной инженерией. Ниже обсудим некоторые идеи по поводу того, как склонить уже имеющихся у вас клиентов к проведению СИ-проверок.

Не предлагайте дополнительные услуги бесплатно

Некоторые наивно полагают, что, если предложить клиентам попробовать услугу бесплатно, они вдохновятся результатом и побегут заказывать ее снова, но уже за деньги. Со мной однажды приключилась история, которая прекрасно иллюстрирует, почему такая тактика не приносит желаемых результатов.

Начиная работать в индустрии технологий и занимаясь сборкой компьютеров, я пытался запустить бесплатный семинар о том, как обезопасить малый бизнес. Больше часа обсуждения я планировал посвятить разбору реальных советов по использованию антивирусов, сетей, файлообменников и т.п. А напоследок заготовил пятиминутную презентацию, с помощью которой хотел убедить представителей компаний обращаться ко мне за соответствующими услугами.

Я заранее договорился с местной торговой палатой об организации бесплатных выступлений. Мы анонсировали три семинара, на которые записалось огромное количество людей: десятки представителей разных компаний на каждый. Я уже начал подсчитывать потенциальные прибыли и чувствовал себя победителем.

И вот настал долгожданный день первого семинара. Я пришел в зал заранее, настроил проектор, разложил на столе раздаточные материалы, которые распечатал на собственные деньги. За пять минут до назначенного времени в зале сидел всего один человек. Как я ни надеялся, что к началу лекции ситуация изменится, этого не произошло. Мне было очень неловко. Я начал свое выступление, но вскоре мой единственный слушатель сказал: «Как-то это странно получается, вам не кажется? Может, лучше сходим пообедать и просто поговорим?».

Я был раздавлен и не мог понять, что же пошло не так. Когда ситуация один в один повторилась на втором семинаре, я понял, что проводить третий бессмысленно, и отменил его. Затем мой друг предложил: «В следующий раз установи цену в $50 за регистрацию. Пообещай дать посетителям информацию, которая стоит намного дороже, — но сначала пусть заплатят».

Мне не хотелось даже пытаться. Я думал: раз никто не дошел до бесплатного семинара, то уж точно никто не будет платить за него. И тем не менее я все-таки решил попробовать. В результате передо мной в зале оказались 10 слушателей, каждый из которых заплатил $50.

ЧТО??? Да, пусть в итоге пришло меньше людей, чем записалось на бесплатную лекцию, но важно другое. Они не просто пришли, но и заплатили за возможность меня послушать.

После проведения семинара я встретился с тем самым другом, который посоветовал брать деньги за выступления. Он объяснил мне, что денежный вклад, пусть даже самый маленький, заставляет людей придавать происходящему большую ценность. Если бы человек записался и не пришел, он бы потерял $50. То есть оплаченная лекция — мотивация к ее посещению.

Но, когда я начал работать в сфере социальной инженерии, оказалось, что на своих ошибках я так и не научился. Мне предлагали выступать с лекциями в разных странах, а я ничего за эти выступления не просил. И часто получалось, что их отменяли или же до последнего момента было непонятно, наберется ли зал.

Моя подруга Пинг Лук посоветовала мне изменить подход и назначить за свое выступление фиксированную цену. Я долго противился этой мысли, но потом вспомнил прошлый опыт и решил попробовать.

И представляете, оказалось, что люди были только рады платить! Меня стали ценить даже больше. В конце концов изменился мой подход к ведению бизнеса: с тех пор я ничего не делаю бесплатно.

Мораль очевидна: не думайте, что люди начнут ценить ваши умения, если вы сами их не цените. Так не бывает. Если вам сложно принять эту мысль, установите скидки на самые дорогие услуги или оформите специальные предложения для клиентов, которые готовы сразу заключить контракт на долгосрочное сотрудничество. Творческий подход к ценообразованию только приветствуется, а вот оказание услуг бесплатно обесценивает ваш труд.

Ошибайтесь и двигайтесь дальше

Иногда при встрече с потенциальным клиентом я понимаю, что он сомневается, надо ли заказывать у меня услуги. Тогда я предлагаю ему начать с разового адресного фишинга, объектом которого станет какое-то влиятельное лицо в его компании. После того как ответственный за принятие решений человек видит преимущества работы с нами и скрытые опасности в случае отказа от этой работы, вопрос о выделении денег на наши услуги снимается сразу же. Однако иногда и этого оказывается недостаточно, клиент уходит.

Как быть, если никак не удается убедить компанию в вашей полезности? Надо смириться и делать следующий шаг. Потерпев неудачу, нужно продолжать движение вперед, а не пытаться снова и снова безрезультатно засовывать кубик в отверстие для шарика.

Если в компании не считают социальную инженерию необходимым элементом системы безопасности, вам с такими клиентами не по пути. С

ними все равно было бы сложно работать, и в результате они, скорее всего, остались бы недовольны вашими услугами.

Например, был у меня клиент, сотрудничество с которым длилось четыре года. Когда мы только начинали совместную работу, он казался мне идеальным заказчиком: мы быстро нашли общий язык, он хотел тут же приступить к действиям. Программа оказалась очень успешной, и изменения не заставили себя ждать. Но вот однажды женщина, которая была нашим контактным лицом в компании и отвечала за реализацию программы, получила от другой организации предложение возглавить их отдел безопасности — и сменила место работы. На ее место пришла новая сотрудница.

С первого дня нашего с ней взаимодействия ситуация изменилась. Она постоянно обижалась, принимала все на свой счет, отказывалась идти на риск и относилась к программе далеко не так серьезно, как ее предшественница. Постепенно программа зачахла. Все вернулось на круги своя, и, хотя статистика по фишингу все еще впечатляла, эффективность программы информирования сотрудников снизилась.

Я понял, что мы потеряем этого клиента, примерно за полгода до того, как наши пути окончательно разошлись. До того случая еще один заказчик ушел от нас подобным образом. Но, думаю, это только к лучшему. Им не хотелось развивать программу в нужном направлении, а это сбивало с толку и их, и нас.

В конце концов, в сутках всего 24 часа, наши физические возможности не безграничны. Поэтому лучше тратить время и силы на тех, кто готов и хочет меняться. Не бойтесь отказываться от неудачных контрактов.

Как определить стоимость своих услуг?

Хотя этот вопрос мне задают очень часто, я не хотел освещать его в своей книге, потому что ответить на него сложно. Но раз уж я взялся за составление этого своеобразного FAQ, совсем обойти такую тему не получится. Так что постараюсь раскрыть ее максимально полно.

Во-первых, разберитесь, сколько в принципе вы можете просить за час своей работы в роли консультанта. Я провел небольшое исследование на этот счет и нашел несколько сайтов, на которых приводилась ориентировочная стоимость услуг специалистов в сфере обеспечения безопасности по всему миру.

Этот показатель зависит от разных факторов: опыта и качества работы, статуса вашей компании, перечня оказываемых услуг.

Теперь давайте подсчитаем. Предположим, я определю стоимость часа своей работы в $100. По предыдущему опыту могу сказать, что фишинг 1000 e-mail в месяц обычно занимает у меня порядка 20 часов. Еще три часа обычно уходит на сбор данных из открытых источников, семь — на

подготовку отчетов. Так что в общей сложности в месяц я потрачу на выполнение работы около 30 часов. Считаем:

30 часов в месяц × $100 в час × 12 месяцев = годовой контракт на $36 000.

Естественно, при работе с разными клиентами цифры варьируются, но примерную стоимость своих услуг я рассчитываю именно таким образом. Цена часа работы может меняться в зависимости от:

- размера компании;
- сроков контракта;
- моего отношения к клиенту (очень субъективный фактор).

Подобные подсчеты помогают рассчитать примерную сумму заказа, хоть и могут оказаться неточными. Однако, по крайней мере, теперь вы представляете, в какую сторону двигаться.

ОБРАТИТЕ ВНИМАНИЕ Этот список вопросов нельзя назвать исчерпывающим. Но разобрать все важные темы в рамках одной книги физически невозможно. Впрочем, я обещаю: если вы напишете мне через форму на нашем сайте https://www.social-engineer.com/contact-us/, я сделаю все возможное, чтобы дать интересующие вас ответы.

Резюме

Однажды мне попался отчет, в котором сообщалось, что лишь небольшой процент работающих в США компаний ежемесячно занимается информированием и обучением сотрудников способам противостояния фишингу.

И тем не менее за последние три года моя компания выросла на 300%. Что же случится, когда 20, 30 а то и 50% американских компаний активно займутся просвещением своих сотрудников?

На самом деле потребность в профессиональных пентестерах, владеющих методами социальной инженерии, просто огромна. Я не могу один ее удовлетворить, поэтому и стараюсь помочь максимальному количеству заинтересованных в этом людей примкнуть к нашему профессиональному сообществу и начать оказывать качественные услуги нуждающимся в этом компаниям.

Не думаю, что наступит время, когда люди вообще перестанут работать. А значит, человеческий фактор будет актуален всегда. Кто-то постоянно будет пытаться использовать нашу эмпатию и страхи, манипулировать нами. От такого давления волей-неволей устаешь и незаметно для самого себя принимаешь неверные решения.

Социальные инженеры всегда будут нужны компаниям для того, чтобы обучать людей противостоять подобным атакам. Наверняка в будущем нам на помощь придут искусственный интеллект и другие технологии, но

не думаю, что наступит время, когда люди смогут обойтись совсем без помощи других людей.

Возможно, вы читаете эту книгу, потому что хотите начать свой путь в мире профессиональной социальной инженерии. Или уже работаете в этой области и надеетесь пополнить профессиональный арсенал новыми приемами. А может, эта книга заинтересовала вас по какой-то другой причине. В любом случае я уверен: следующая глава будет вам особенно интересна, потому что благодаря ей вы сможете создать собственный план минимизации и предотвращения последствий.

10

Есть ли у вас ПЛАН?

> Я верю в необходимость контролировать то, что можно контролировать; забывать то, что контролировать нельзя; и не тратить энергию на вещи, которые этого не заслуживают.
>
> Джош Цитрон

Книга, посвященная привлечению новых специалистов в мир профессиональной социальной инженерии, пожалуй, не была бы полноценной без этой главы. Результатов можно достичь, если изучить типы атак и лежащие в их основе психологические и физиологические принципы, а также если набить руку в написании отчетов — но если отсутствует ПЛАН, все равно будет не хватать чего-то очень важного. Что такое ПЛАН? Это план минимизации и предотвращения последствий (ПМиП).

Зачем его составлять и как помочь клиентам это сделать? О минимизации каких последствий можно говорить в контексте социальной инженерии? Ответы на эти вопросы вы найдете ниже.

Когда я только начинал свой профессиональный путь, то понял нечто очень важное: мне нужно было достичь довольно странной цели — работать настолько профессионально, чтобы клиентам больше не нужны были мои услуги. Да, вы все верно поняли. Я стремился обучать клиентов защищаться от социальных инженеров настолько хорошо, чтобы они больше не нуждались в услугах сторонних специалистов.

Вам наверняка попадалась реклама компаний, занимающихся пентестингом и хвастающих тем, что их проверки всегда успешны на 100%? Представляете, как клиента, выписывающего вам чек, должна демотивировать мысль о том, что лучше никогда не станет: как бы они ни старались, социальный инженер все равно окажется на шаг впереди! Подобные слоганы сообщают клиентам, что надежды нет. Какие бы усилия они ни прикладывали, дыры в системе безопасности не залатать ничем. Если рассуждать таким образом, становится ясно, почему некоторые клиенты не понимают, «зачем вообще что-то делать».

И вот когда до меня это дошло, я решил, что всегда буду помогать клиентам готовить план минимизации возможных последствий подобных атак, а также их предотвращения. Чтобы со временем у них отпала потребность заказывать у меня проверки, потому что останется только совершенствовать уже имеющиеся навыки. Если вы придерживаетесь тех же убеждений, эта глава будет очень важна для вашего профессионального успеха. Ну а если вы из лагеря клиентов, она поможет вам составить собственный ПМиП.

Я окончательно убедился в необходимости ПЛАНа, когда понял, что нужно заняться своим здоровьем. Попытки самостоятельно улучшить физическое состояние с треском провалились. Однако в сообществе добрых хакеров у меня было несколько знакомых, которые добились успеха в этом нелегком деле. Я спросил одного из них, как ему удалось взять себя в руки. И тот связал меня с человеком по имени Джош Цитрон.

Джош предложил провести первую консультацию по видеосвязи. Меня эта идея не вдохновила: я знал, что он находится в идеальной физической форме, и мне совсем не хотелось видеть свою толстую тушку рядом с его подтянутой фигурой. Ситуация только усугубилась, когда я нашел в интернете его фотографии (это было не сложно). Он оказался не просто подтянут — передо мной предстал один из тех супергероев, которые, знаете, могут голыми руками поднять машину и пробежать с ней 5 км.

И представьте, что бы произошло, если бы на первой же встрече с Джошем (а она все же состоялась) я услышал от него такие слова: «Крис, если вы будете следовать каждому моему совету, слушать каждое мое слово, исправно мне платить и при этом не мухлевать… у вас все равно ничего не получится. Вы будете толстым и слабым всю жизнь. Ну что ж, начнем?» Скорее всего, я бы подумал, что он не в себе. А если бы он смотрел на меня надменно или демонстрировал плохое ко мне отношение (ведь выгляжу-то я не очень), я бы вряд ли стал с ним работать.

Однако Джош поступил по-другому. Он пообещал: если я буду выполнять все его указания, через какое-то время начну замечать постепенные изменения. А после достижения поставленных целей смогу самостоятельно поддерживать результат. При этом он обращался ко мне очень уважительно, так что по итогам беседы я был готов действовать.

По большому счету, Джош помог мне составить ПЛАН в отношении старых вредных привычек и освоении новых, более полезных. Мы не говорили о радикальных диетах, в которых отсутствуют продукты, обладающие хоть каким-то вкусом: типа на ужин — только салаты и грусть. С ним я перестроил привычки и научился принимать более эффективные решения.

То же самое применимо и к социальной инженерии. Я сформулировал четыре основных шага, которые помогают создать качественный ПЛАН и пользоваться всеми его преимуществами:

- Шаг 1: научиться выявлять СИ-атаки.
- Шаг 2: разработать реализуемые и реалистичные правила для сотрудников.
- Шаг 3: проводить регулярные проверки.
- Шаг 4: реализовывать программы информирования сотрудников по вопросам безопасности.

И я обещаю: если вы выполните каждый из перечисленных шагов, необходимые изменения на уровне корпоративной культуры действительно произойдут. Конечно, не мгновенно (скорость осуществления изменений зависит от множества факторов: количества задействованных сотрудников, текущего состояния корпоративной культуры и прочего). Процесс может занять даже несколько лет — но изменения на самом деле будут.

Ну что, вы готовы?

Шаг 1: научиться выявлять СИ-атаки

В юности мне очень хотелось научиться драться, поэтому я взялся изучать боевые искусства. Помню, как познакомился с тренером. В качестве пробного занятия он предложил мне попробовать блокировать его удары. Мне тогда показалось, что его кулаки буквально материализуются в воздухе и тут же оказываются у разных частей моего тела.

К счастью, он не бил меня, а только слегка похлопывал. Тем не менее у меня ни разу не получилось остановить его нападение. Но прошел год занятий, и мне уже удавалось блокировать большую часть направленных в мою сторону ударов. Что изменилось? Я научился распознавать разные типы ударов, и это позволило мне правильно на них реагировать.

Первый шаг кажется очевидным, но он далеко не так прост. Как думаете, какой процент сотрудников вашей компании сможет объяснить, что такое фишинг, вишинг, SMiShing и имперсонация? Сколько из них расскажут, почему опасно разглашать название компании, занимающейся ремонтом мусорных баков и вывозом мусора? Кто разбирается в механизмах работы вирусов, программ-вымогателей и «троянов»?

Поймите меня правильно: я не утверждаю, что каждый ваш сотрудник должен стать Брюсом Ли социальной инженерии. Но он должен знать, о чем идет речь и чем опасна неосведомленность. И первый шаг к пониманию разных векторов атак — научиться узнавать их и понимать их последствия.

Полагаю, вы сейчас задаетесь вопросом о том, как же это сделать. Верно мыслите. Если бы много лет назад, когда я впервые пришел в школу боевых искусств, тренер сказал мне: «Хочешь научиться драться? Вон маты, а вон мастер, который занимается уже 20 лет. Сразись с ним, и все поймешь!» — я бы тут же смылся. Если бы он посадил меня перед экраном, включил 20-минутное обучающее видео, а после просмотра отправил меня на додзё, моя реакция не сильно изменилась бы. (Опустите вилы, я не говорю, что обучающие видео бесполезны. Это прекрасный инструмент, и ниже мы обсудим его подробнее. Однако, сделав его основным элементом программы, вы допустите серьезную ошибку.)

Мой тренер научил меня видеть поле боя и держать удар — то же самое должен сделать для компании социальный инженер. В школе боевых искусств меня сначала учили принимать правильное положение тела и грамотно двигаться. Потом я перешел к тренировкам с грушей. И лишь после того, как тренер решил, что я готов к реальному бою, я приступил к спарингу с живым противником. Но этот противник не пытался меня убить — он тоже помогал мне учиться.

Навык распознавания СИ-атак даст вам огромную фору по сравнению с несведущими в этих вопросах людьми. Помогите своим сотрудникам осознать истинную ценность информации — о том, что подорвать безопасность компании можно с помощью одного-единственного e-mail; что мошенники умеют получать пароли и другую важную информацию по телефону; что их мобильные устройства могут подвергаться атаке и в дальнейшем использоваться для подрыва индивидуальной и корпоративной безопасности; что дружелюбная улыбка посетителя не повод для нарушения пропускной политики.

Рассказывая своим сотрудникам о возможных векторах атаки, вы формируете их осведомленность. Я сам постоянно варюсь в этой теме, поэтому иногда забываю, что большинство людей даже не догадываются о существовании опасности.

Однажды друг рассказал мне, как его бабушка вложила огромную сумму денег в MoneyGram: кто-то позвонил ей якобы от лица одного из внуков и сказал, что срочно нуждается в деньгах. Я воскликнул:

— Как жаль, она стала жертвой известного бабушкиного развода.

— Чего-чего? — не понял друг.

Я объяснил, что, к моему большому сожалению, этот тип мошенничества весьма распространен. На что друг возмутился:

— Раз ты о нем знаешь, чего же друзей не предупредил?

И он был совершенно прав! Я почему-то предполагаю, что все вокруг читали или слышали о подобных схемах. Но это не так. Конечно, невозможно угадать, действительно ли мои рассказы помогли бы им. Кто знает. Но тем не менее выводы я сделал.

Вернемся к моему тренеру Джошу. После нашей первой видеовстречи я раз в неделю отправлял ему свои отчеты. Придерживаться программы мне удавалось не всегда. И знаете, чего он никогда не делал? Не отчитывал, как ребенка, не обвинял, не отмахивался от меня. Он просто говорил: «Что ж, на следующей неделе постарайся справиться лучше».

Возьмите себе на заметку и пользуйтесь. Не рассчитывайте на то, что все вокруг имеют представление о социальной инженерии. А если у людей нет необходимых знаний, это не значит, что они глупые, тупые и поэтому должны попасться на крючок мошенников. Проявите эмпатию. Скажите: «Что ж, постараемся в следующий раз сделать лучше. Как думаете, что для этого нужно сделать?» Такой подход поможет намного успешнее справиться и со следующим шагом.

Шаг 2: разработать реализуемые и реалистичные правила для сотрудников

Один из первых навыков, которые я освоил благодаря Джошу, заключался в понимании того, как должна выглядеть нормальная порция еды. Он рассказал мне, сколько белков, жиров и углеводов я должен потреблять в течение для. А дальше решение было за мной: можно было съесть все это хоть за один присест — но тогда я бы точно проголодался позже.

Кроме того, Джош научил меня не доверять глазам. Как-то раз он предложил выложить на тарелку то количество еды, которое казалось мне правильным. А затем взвесить ее. Разница между моими представлениями о нормальном размере порции и реальностью оказалась КОЛОССАЛЬНОЙ. Именно требование взвешивать еду перед ее употреблением позволило мне понять, что именно необходимо изменить в своих привычках.

В мире безопасности такие правила превращаются в «политику компании». Это словосочетание обычно имеет какие-то негативные коннотации. Многие руководители ненавидят разрабатывать и внедрять ее, а многие сотрудники не любят ей следовать. По моим наблюдениям, дурная репутация словосочетания связана с тем, что зачастую политика компании по тем или иным вопросам формулируется размыто, непонятно. Или же это настолько строгие правила, что в их исполнении люди видят больше вреда, чем пользы.

Найти необходимый баланс бывает сложно, но это необходимо сделать, если вы хотите создать в своей компании безопасную среду и сформировать культуру осведомленности.

Как же разрешить это противоречие? Как разработать не слишком строгую и реалистичную политику безопасности, которой было бы просто придерживаться? Давайте разберем несколько рекомендаций, которые

помогут вам разработать четкие правила для сотрудников и улучшить текущую ситуацию.

Вынесите размышление за пределы уравнения

Многие правила сформулированы слишком обтекаемо и широко. То есть исполнителю приходится делать выводы и даже принимать решения, исходя из собственных соображений. А ведь на месте такого исполнителя вполне может оказаться человек, даже не представляющий, какие формы способна принимать СИ-атака. Я не предлагаю вам относиться к сотрудникам как к дурачкам. Просто запомните: чем меньше исполнитель будет думать о том, что ему нужно сделать, тем лучше. Понятные правила работают эффективнее всего.

Приведу пример из практики. Моя компания проводила вишинг для крупной финансовой организации, и в 80% случаев мы успешно собирали необходимые персональные данные. Мы делали ставку на эмпатию, доверие и получали желаемое.

Справедливости ради нужно отметить, что в компании работали действительно приятные и добрые люди. Мы не хотели этого менять. Только представьте себе такой совет по минимизации негативных последствий для руководства: «Доведите ваших сотрудников до паранойи, пусть не доверяют никому». Мы, конечно же, такого не советовали. А руководители компании приняли по-настоящему мудрое решение. Они сформулировали новое, простое, выполнимое правило: «Запрещено сообщать какую бы то ни было личную информацию пользователям, не прошедшим процедуру аутентификации».

Но и на этом руководство не остановилось. С сотрудниками провели разъяснительную работу о том, какая информация считается особенно ценной и как правильно организовывать ту самую аутентификацию пользователей. Наконец, «наверху» приняли еще одно решение, которое и определило успех новой политики: лишили сотрудников возможности получения доступа к информации без идентификации пользователя. Это выглядело так.

Атакующий: Добрый день. Меня зовут Джон Смит. Мне нужна информация по моему аккаунту, а я забыл пароль. Могли бы вы помочь мне восстановить его?

Сотрудник: Безусловно. Чтобы это сделать, мне нужно будет подтвердить вашу личность. Скажите, пожалуйста…

Дальше сотрудник должен был задать пользователю ряд вопросов и вводить ответы в специальные графы. Доступ к запрашиваемой информации открывался только после корректного ввода всех необходимых данных.

После внедрения новой политики мы организовали ряд образовательных мероприятий, а затем снова запустили проверку. Благодаря новым

правилам и знаниям, которые получили сотрудники, их система безопасности стала непреодолимой. Люди остались такими же добрыми и человечными, здесь ничего не изменилось (в ходе контрольной проверки десятки человек искренне расстраивались, когда не могли мне помочь, хотя действительно делали все возможное). Однако изменения в политике компании и повышение осведомленности персонала позволили устранить сомнения в том, как правильно поступать, чтобы защитить безопасность компании.

Устранить возможность нарушений по причине эмпатии

Обратите внимание: это не совет «избавиться от эмпатии». Я бы такого никогда не предложил. Речь идет о том, что сотрудникам нельзя игнорировать корпоративные правила, руководствуясь эмпатией.

У меня в Англии есть хорошая подруга, Шерон Конхэди. На позднем сроке беременности ей довелось проводить проверку безопасности. И она использовала свое положение как способ пробудить в объектах воздействия эмпатию.

Она взяла коробку, наполненную разным хламом, чтобы та выглядела тяжелой, и поволокла ее прямо ко входу. Мужчины, обращавшие внимание на ее страдания, тут же бросались на помощь. Они заносили эту коробку в здание и провожали Шерон прямо в серверную. Ни один не попросил показать бейджик или пропуск: ведь преступники не беременеют, верно?

Безусловно, мужчины совершали хороший поступок — помогали беременной женщине. Разве можно заставлять людей отказываться от заботы о ближнем? И компания не стала так делать. Вместо этого она организовала информационную кампанию, нацеленную на то, чтобы объяснить сотрудникам: помогать ближним важно и нужно, однако при этом нельзя забывать проверять пропуск, прежде чем пропускать незнакомцев в здание.

Просто сказать «Проверяйте пропуска» было бы недостаточно. Ведь эмпатия возникает благодаря старой доброй «миндалине» — того самого отдела мозга, который способен отключать центры логики и заставлять нас принимать сугубо эмоциональные решения. Информирование, напоминания и четкие инструкции позволяют защитить сотрудников от манипуляций эмпатией и тем самым добиться выполнения требований безопасности.

Реалистичные и реализуемые требования

Я собственными глазами видел такую формулировку в требованиях безопасности одной компании: «Не переходите по опасным ссылкам».

Как вам? Если вы думаете: «Отличное правило, пожалуй, я им тоже воспользуюсь», рекомендую закрыть эту книгу и пару раз стукнуть ею себя по голове.

Теперь можно читать дальше.

Подобные требования плохи тем, что они недостаточно подробны. Как понять, какие ссылки опасны? Знают ли сотрудники, что сайты support-microsoft.com и Microsoft.com — это совершенно разные вещи?

Кроме того, в этой формулировке не прописаны возможные последствия нежелательного действия. А если перейти по ссылке, то что произойдет? Было бы полезно дополнить это правило формулировкой в духе: «Если же нежелательное взаимодействие с электронным письмом, подозрительный телефонный разговор или личное взаимодействие все же состоялись, пожалуйста, сообщите о сложившейся ситуации на xxxxxxx@company.com».

Но и этого недостаточно! Необходимо объяснить сотрудникам, что именно им надо сообщить: переслать сомнительное письмо, приложить информацию о звонившем человеке и т.п. Какую именно информацию вы хотите получить? И какие последствия ждут сотрудника, который предоставит вам такой отчет?

Реалистичная политика безопасности помогает сотрудникам оценивать возникающие ситуации со всех сторон. У них просто не остается вопросов. Однажды меня попросили поучаствовать в подготовке информации для увеличения осведомленности сотрудников в вопросах фишинга. Текст был примерно следующий:

Фишинг — серьезная угроза лично для вас и для компании в целом. Мошенники хотят получить от вас конфиденциальную информацию и добиваются этой цели в том числе с помощью атак через электронную почту. Они могут отправить вам зараженные документы с расширением .exe, .pdf, .xls, .doc. Кроме того, они могут прикладывать к письмам ссылки на сайты, которые на самом деле являются лишь ширмой для распространения вредоносных программ и вирусов.

Получив e-mail от непроверенного отправителя, не предпринимайте в отношении него каких бы то ни было действий, только перешлите его на адрес нарушения@компания.com (нажмите кнопку «Переслать» в шапке вашего почтового ящика»).

В течение суток вы получите ответ с оценкой безопасности этого письма.

Если же вы перешли по ссылке или открыли документ, который теперь кажется вам подозрительным, — сообщите об этом в отдел по контролю за нарушениями.

Конечно же, полная версия руководства содержала более подробное описание новой политики безопасности, а также ссылки на дополнительные информационные ресурсы. Но я думаю, суть вы понимаете. Хорошая политика безопасности всегда предлагает

реалистичные инструкции и формирует у сотрудников четкие представления о том, какие действия нужно совершать, а какие не нужно.

Возвращаясь к моему примеру с боевыми искусствами: этот шаг можно сравнить с обучением «новобранцев» принимать правильную позу, держать руки и грамотно следить за действиями противника — конечно же, с разъяснением значения этих действий. Хорошая политика безопасности сообщает сотрудникам, «что» надо делать и «почему». Если составить ее правильно, у людей из вашего штата со временем сформируется стойкая память на такие вещи.

Вот тогда-то и можно будет перейти к следующему шагу.

Шаг 3: проводить регулярные проверки

Каждую неделю я отправлял Джошу отчет о потребленных калориях, сделанных упражнениях, часах сна, колебаниях веса и других подробностях жизни своего тела. Каждый день я все это записывал с мыслью о том, что Джош будет оценивать мои результаты. Регулярные проверки помогали мне не сбиться с верного пути и помнить о своей цели, а Джош в свою очередь получал возможность вовремя выявлять всяческие проблемы этого процесса.

И вот наступила неделя, когда мне пришлось много путешествовать: вести подробные отчеты возможности не было, я записывал наугад. Джош тут же заметил несоответствие между данными и результатами и задал мне несколько вопросов, которые помогли выявить проблему, решить ее и двинуться дальше. Теперь вы понимаете, чем эффективные программы отличаются от неэффективных: регулярными проверками.

Итак, вы уже рассказали своим сотрудникам о том, какие бывают атаки. Объяснили им, как действовать в случае, если в роли объектов такой атаки окажутся они сами. Вы разработали правила, которые помогут им принять грамотные решения в сложной ситуации. А теперь пришло время проверить, была ли эта информация усвоена. Сработает ли «мышечная память», когда человек окажется под давлением обстоятельств в ходе проверки? Единственный способ это узнать — пригласить консультанта по безопасности на образовательный спарринг с этим сотрудником.

И выбор консультанта здесь крайне важен. Если вы, дорогой читатель, сами являетесь социальным инженером и хотите найти себе клиентов, прочитайте эту часть особенно внимательно, чтобы узнать, чего хотят получить от вас компании. Помните: вам не нужно добиваться стопроцентных показателей или взламывать все, что попадется на пути. Ваша цель — применить свои знания, чтобы заказчик смог усовершенствовать систему безопасности в своей компании.

Итак, как же выбрать специалиста, подходящего для решения этой задачи?

Задавайте правильные вопросы. Не стесняйтесь: просите рассказать, какие заказы он выполнял ранее и что рекомендует делать для решения интересующих вас вопросов. Совпадают ли ваши представления на этот счет?

Например, однажды я консультировал компанию, представитель которой спросил, что я предлагаю делать с сотрудниками, которые в ходе проверки поступят неправильно. Я ответил честно и просто, что считаю первостепенной задачу обучения людей. А значит, такому сотруднику нужно показать и объяснить его ошибки. А потом снова подвергнуть проверке. Лишь после этого можно будет сделать вывод о том, представляет его поведение угрозу для организации или нет. Я также сказал, что считаю систематическое увольнение людей по результатам пентестов плохой идеей. Такой ответ соответствовал и представлениям компании, поэтому мы продолжили сотрудничество.

На первых организационных встречах меня часто просят описать конкретные сценарии атак, которые я собираюсь осуществить. Обычно я отвечаю, что сначала должен провести сбор данных из открытых источников и лишь после этого смогу разработать верную стратегию. Тем не менее я обязательно привожу в пример проекты, которые осуществлял раньше в компаниях похожего профиля.

Так что если вы являетесь представителем компании в поисках подходящего социального инженера, задавайте хорошие вопросы. А если вы социальный инженер — старайтесь с толком на них отвечать.

Отзывы. Найти компанию, готовую посоветовать вам проверенного специалиста, может быть сложно, потому что многие предпочитают скрывать факт заказа СИ-услуг. Одна из причин этого — в том, что в процессе подрыва системы безопасности злоумышленники зачастую используют знания о компаниях-подрядчиках, сотрудничающих с объектом. Я договорился с несколькими клиентами о том, что буду приводить их пример будущим заказчикам. И, по-моему, это помогает мне представить себя в правильном свете. Новые заказчики получают возможность узнать у третьих лиц, каково это на самом деле — сотрудничать с заинтересовавшим их специалистом.

Помните: ни один социальный инженер не будет приводить в пример заказчика, который остался недоволен сотрудничеством. Тем не менее изучение отзывов позволит вам составить представление о специфике работы специалиста и качестве оказываемых им услуг.

Четко определите правила. Самая неэффективная для клиента стратегия поведения — думать, что пентестер ограничится одним уровнем проверки. А когда выяснится, что он пролез в самые недра компании, вам придется объяснять начальникам, как вы это допустили. Избежать подобных проблем можно, если заранее определить границы,

заступать за которые недопустимо. По сути, такие правила выполняют функцию защитной экипировки, которую используют во время боя боксеры.

Наверняка у вас найдутся и свои специфические требования к пентестеру. Однако эти три пункта помогут сориентироваться и найти наилучшего исполнителя для решения такой задачи.

А когда вы его найдете, результаты проверки помогут понять, какие еще услуги вам понадобятся и как часто нужно будет проводить дополнительные тесты. Хороший специалист поможет вам определиться с ответами на эти вопросы и будет ориентироваться на истинные потребности вашей компании (а не на собственную потребность увеличить количество нулей в чеке).

Некоторые услуги лучше заказывать раз в месяц (например, фишинг). Другие формы тестов можно проводить раз в год или в полугодие (например, полноценные пентесты). Универсального решения, подходящего для всех, просто не существует. Во многом оно зависит от ваших потребностей и представлений о том, как вы хотите достичь поставленных целей.

Наконец, вам остается сделать последний, четвертый шаг.

Шаг 4: реализовывать программы информирования сотрудников по вопросам безопасности

Джош публикует видеозаписи, где демонстрирует правильное выполнение упражнений. Он рассказывает и показывает, как сам бегает и занимается другими полезными для здоровья вещами. Такие видео представляют собой отрывки информации, которая помогает его ученикам понимать, зачем они делают то, что делают. Такой же принцип можно применять и при подготовке программ повышения информированности в вопросах безопасности.

Возможно, вы сейчас недоумеваете: «А разве предыдущие три шага не рассказывали о том, как должна действовать такая программа? Кажется, автор забылся и повторяется». Вообще-то нет. Все описанные выше шаги, безусловно, являются частью создания такой программы, но последний шаг целиком и полностью посвящен ее практическому воплощению.

Для наглядности позвольте привести очередной пример из собственной практики. Был у меня клиент, который сразу заказал большое количество тестов. Моя команда провела качественный сбор данных из открытых источников, а затем мы занялись вишингом и фишингом.

Но сотрудники его компании продемонстрировали какую-то сверхъестественную невосприимчивость к нашему вишингу. Они не выдавали ничьих имен, телефонных номеров и даже отказывались подтверждать, кто на момент звонка находился в офисе. А вот во время фишинга обнаружилось множество слабых мест.

Анализ мер, которые уже принимались в компании, показал, что информирование проводилось по обоим направлениям. Однако вишинг разбирали намного подробнее: сотрудникам рассказывали про атаки, описывали реалистичные сценарии, предлагали конкретные меры противодействия и регулярно проверяли их соблюдение.

А часть программы, посвященная фишингу, состояла из ежегодного просмотра нескольких видеороликов. Я мог бы попытаться продать клиенту новые программы по защите от вишинга и фишинга, но ему это было просто не нужно. Поэтому мы сосредоточились на доработке части программы, посвященной фишингу. Я призвал клиента ничего не менять в отношении вишинга. Короче говоря, я помог ему понять, какие доработки необходимы, ориентируясь на результаты, полученные в процессе выполнения предыдущих трех шагов.

Одинаковых клиентов не бывает, каждый заказ уникален. Поэтому создание действительно готовых к реализации программ занимает определенное время. Этот процесс нельзя свести к использованию заготовок и созданных заранее модулей.

Разрабатывая программу повышения осведомленности, отвечающую конкретным потребностям конкретного клиента, вы помогаете сотрудникам его компании понять, что не нужно и что нужно делать, если ситуация будет развиваться по нежелательному сценарию. Вы помогаете разобраться в новой политике безопасности, а затем придерживаться ее.

А вот еще один пример из моей работы с Джошем. Когда он советовал мне снижать потребление определенного вида пищи или чаще заниматься определенными активностями, я был готов следовать его рекомендациям, даже если они мне не нравились. Почему?

- Я видел позитивный эффект — изменения, происходившие со мной под его руководством.
- Джош подробно и понятно объяснял, что и зачем мне нужно делать.
- Он давал мне реалистичные советы по преодолению возникающих трудностей.
- Когда я терпел неудачу (а это случалось нередко), Джош не называл меня лузером (а я таковым себя чувствовал). Он действовал ровно наоборот: относился ко мне как к человеку, которому нужна помощь и который стремится найти способ в следующий раз не наступить на прежние грабли.

Его программа помогла мне не только улучшить состояние здоровья, но и сделать важные выводы по поводу того, как внедрять в компаниях новые требования безопасности. Не думайте, что если вы все поняли, то ваши знания автоматически передадутся всем сотрудникам. Им может потребоваться больше времени, чтобы разобраться.

Соединяем все вместе

Вспомните те далекие времена, когда в смартфоны еще не встраивали всевозможные дополнительные функции, в том числе карту всего мира с GPS-навигацией. Припоминаете? Я — да.

Когда-то я даже пользовался бумажными картами. И делал это по принципу выполнения все тех же четырех шагов.

Шаг 1 (научиться выявлять атаки) — найти свое место на карте. После этого я искал самый короткий маршрут, который не предполагал проезда по платным или небольшим дорогам, но в то же время приближал меня к пункту назначения.

Шаг 2 (разработка реализуемых и реалистичных правил) — проложить маршрут таким образом, чтобы захватить максимальное количество скоростных шоссе, на которых можно двигаться быстро.

Шаг 3 (проводить регулярные проверки) — я периодически уточнял, на какой именно нахожусь дороге, и сверялся с проложенным на карте маршрутом, чтобы ничего не перепутать.

Наконец, шаг 4 (программа информирования) объединял весь процесс использования карты: я вовремя добрался из пункта А в пункт Б, не попадая в неприятности, — одним словом, действовал в соответствии с собственным планом.

Карта помогала мне передвигаться по США в реальной жизни, так же как ПЛАН помогает ориентироваться в вопросах создания программ безопасности.

Обратите внимание: недостаточно было бы ограничиться только первым шагом или просто положить в машину карту и ждать магического перемещения в пункт назначения. Нет. Нужно сначала составить план, а потом воплотить его в жизнь.

Конечно же, я не могу пообещать каждому из вас волшебного превращения в супергероя Мистера Безопасность. Тем не менее выполняйте эти четыре шага, и вы сможете развить необходимые для отражения атак мускулы.

В оставшейся части главы мы разберем еще несколько важных аспектов, которые необходимо иметь в виду при разработке ПЛАНа.

Обновляйтесь

Предположим, вы успешно выполнили четыре шага. Можно ли с чистой совестью вешать на дверь бумажку с печатью и подписью: «Защищено от хакеров»?

Можно, конечно, если хотите повеселить мошенников, которые будут в эту дверь входить. Выполнение описанных выше шагов сделает вас не самой легкой мишенью и поможет подготовить сотрудников к возможным атакам. Это, безусловно, полезная практика. Но она не защитит вас от риска подвергнуться фишингу, вишингу, CMC-мошенничеству или имперсонации — и попасться на уловки злоумышленников. Что же делать?

Ответ прост: нужно постоянно обновлять компьютерные программы. Невозможно сосчитать, сколько раз в ходе рутинной проверки безопасности я обнаруживал, что в компаниях массово используются браузеры, устаревшие аж на три версии, программы для просмотра PDF-файлов, почтовые программы и даже операционные системы (!). В старых версиях обычно больше уязвимостей. Только регулярные обновления системы защитят вас от атак и взломов, связанных с использованием устаревшего программного обеспечения.

Я прекрасно понимаю, что советовать намного проще, чем делать. Я знаю, что на постоянные обновления нужно тратить время, силы и деньги. Тем не менее не стоит забывать, что в 2017 году подрыв системы безопасности обходился компаниям в среднем в $3,62 млн. В среднем! А самые громкие атаки наносили ущерб в $10–300 млн!

Я не настолько наивен, чтобы полагать, будто регулярные обновления спасли бы всех жертв подобных атак. Я просто предлагаю вам сопоставить стоимость профилактики (защиты) и стоимость устранения их последствий. Впрочем, если безопасность ассоциируется у вас с образами в духе изображенного на илл. 10.1, нам, пожалуй, стоит обсудить этот вопрос более серьезно.

Можно закопать голову в песок и надеяться, что хищники вас не заметят. Но толку? Когда платить: до атаки или после — решать только вам. Лично я считаю, что намного логичнее заранее тратить время, деньги и напрягаться, защищая тем самым своих клиентов и репутацию, а не разгребать последствия позора и скандалов.

Учитесь на ошибках коллег

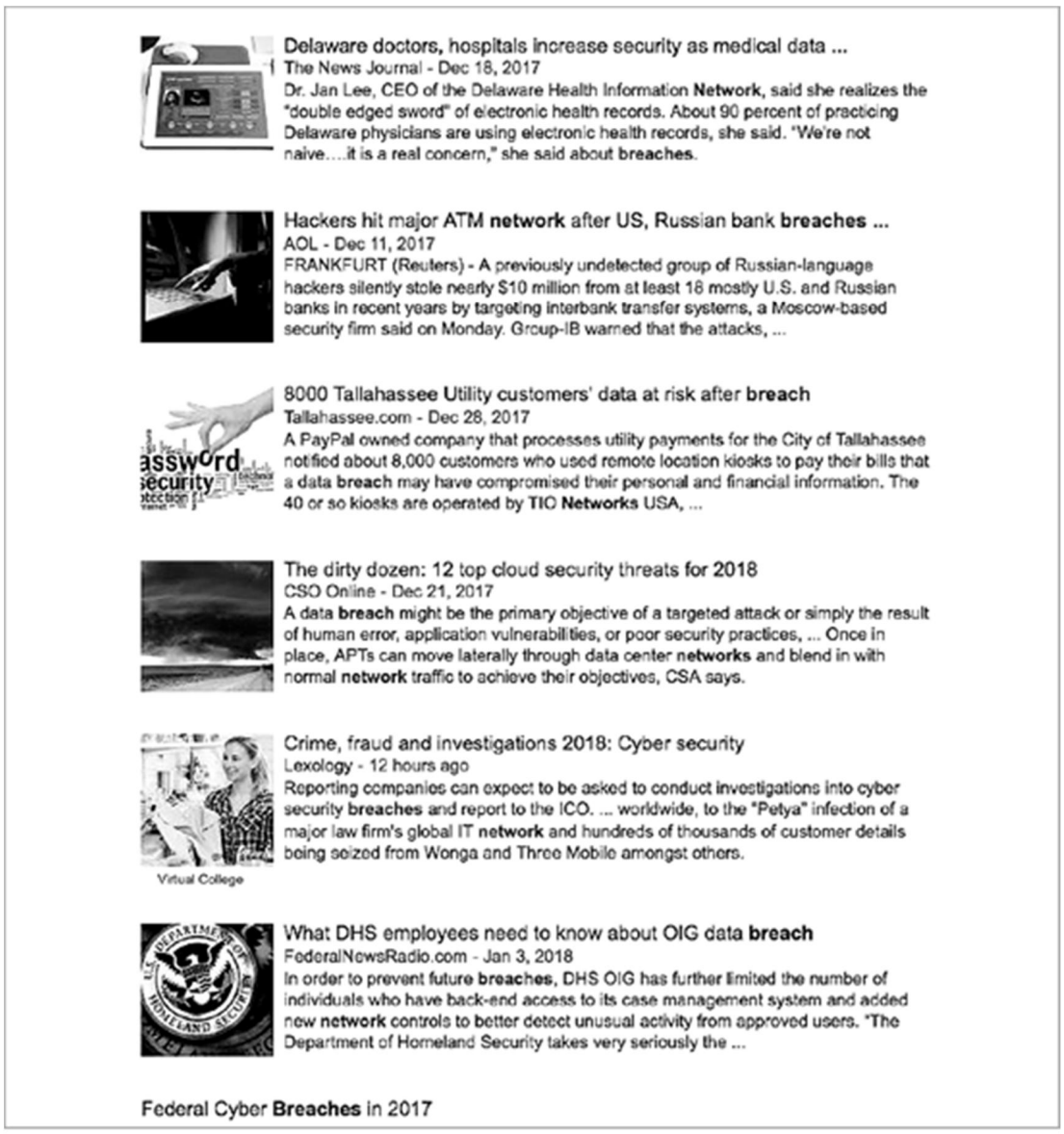
Откройте Google, введите в поисковую строку запрос «Брешь в безопасности» и выберите раздел «Новости». На скриншоте 10.2 вы видите результаты, которые я только что получил.

В этих статьях описаны подробности и причины произошедшего, действия злоумышленников и конкретные уязвимости (со стороны людей, программ или техники), которыми они воспользовались. Если вы

научитесь разбираться, почему другие пали жертвой подобных атак, то сможете позаботиться о безопасности своей компании.

Илл. 10.1. Безопасность выглядит не так

Узнав, что против какого-то файервола успешно использовали определенный эксплойт, имеет смысл проверить, какой файервол установлен в вашей сети и устранена ли в нем эта уязвимость. Увидев новость о компрометации корпоративной электронной почты через определенную форму фишинга, усильте меры информирования сотрудников по этим вопросам и проверьте эффективность исполнения соответствующих распоряжений. Короче говоря, любое попавшее в новости событие должно стать для вас полезным уроком и подтолкнуть к актуализации знаний о грозящих опасностях и необходимости обновления инфраструктуры, если в ней выявлены уязвимости.



Илл. 10.2. Пример актуальных новостей

Существуют разные компании, предлагающие услуги по моделированию уязвимостей. Возможно, вам имеет смысл обратиться к ним. Или же начать делать это самостоятельно — чтобы корректировать, укреплять и обновлять существующие программы и протоколы в соответствии с актуальными опасностями.

Создайте культуру бдительности

Чтобы проиллюстрировать этот пункт, я снова расскажу о том, как работал с Джошем. Мы выяснили, какие ситуации и формы моего поведения мешают прогрессу. Например, мелочи вроде отказа от подсчета калорий и взвешивания порций приводили к замедлению прогресса. А если я заходил в пиццерию на шведский стол, убеждая себя, что остановлюсь после пары кусочков, обычно случались серьезные срывы.

Джош помог мне понять, что здоровый образ жизни складывается из маленьких ежедневных решений. Мне вовсе не обязательно съедать полкило стейка, чтобы наесться: достаточно 200 г филе. А если я собираюсь заказать на ужине в ресторане десерт, то стоит с умом подходить к приемам пищи, начиная с самого завтрака, и к концу дня удержаться в собственных рамках. И так далее.

Какое отношение все это имеет к корпоративной культуре осведомленности в вопросах безопасности? Да самое прямое!

Если должным образом готовить сотрудников, регулярно напоминать им о необходимых мерах безопасности и поощрять следование протоколу, то со временем в компании сформируется соответствующая культура. Каждый сотрудник будет знать, что любое его мелкое решение может иметь долгосрочные последствия. И каждый будет знать о том, какой вред компании могут нанести более серьезные ошибки с его стороны.

Благодаря работе с Джошем я сбросил вес, стал лучше себя чувствовать и выглядеть, мое здоровье окрепло. Эти улучшения вдохновили меня продолжать работу. Однако не каждый сотрудник будет так же мотивирован, если «раскусит» фишинговый e-mail или «сообщит» о случае вишинга. Не потому, что ему все равно, не потому, что он ненавидит компанию. Просто у него может быть слишком много других дел и обучающие программы будут казаться ему бесполезной тратой драгоценного времени.

С таким настроем сотрудников работать сложно— но возможно. Например, однажды мне довелось работать в организации, где менеджер отдела однозначно и открыто продемонстрировал свое негативное отношение к нашей деятельности. В результате 450 его подчиненных превратились в главное уязвимое место компании. В его отделении постоянно возникали проблемы с вирусами, фишингом и другими формами атак.

Руководитель понял, что его сотрудники попросту не выполняют требований безопасности. Он не знал, что делать, и пытался исправить ситуацию через наказание виноватых. Лично я ни разу не видел, чтобы такой подход работал: обычно он, наоборот, лишь усиливает напряжение в отношениях между начальником и подчиненными. Если сотрудники все же следуют протоколу в таких ситуациях, то делают это со страхом, злостью и презрением. Поэтому в ходе очередной встречи с клиентом я предложил провести среди работников его колл-центра шуточный конкурс. В качестве приза взять мягкую игрушку в форме рыбы. А первый сотрудник, который не перейдет по вредоносной ссылке и сообщит о фишинговой атаке руководителю, получит эту игрушечную рыбу на свой рабочий стол и заработает статус «Главного фишера»[18] на целый месяц.

Возможно, вы сейчас сидите и думаете, что это дурацкая идея. Согласен. Тем не менее два месяца спустя 450 взрослых сотрудников

сражались за то, чтобы заполучить игрушечную рыбу. А званием «Главного фишера» по-настоящему гордились.

В результате существенно увеличилось количество людей, активно вовлеченных в программу. Сотрудники искали «плохие» письма, и количество сообщений о них за несколько месяцев возросло с 7 до 87%. Количество переходов по опасным ссылкам за то же самое время сократилось с 57 до 10%. Но самое главное, объем вредоносного кода, выявляемого в Сети, снизился более чем на 79%.

Одна простая мера позволила изменить отношение к безопасности в компании. Сотрудники начали принимать более грамотные решения, увидели последовавшие за этим изменения и ощутили мотивацию их поддерживать.

Как добиться таких же изменений в вашей организации? Без личной беседы с вами я точно на этот вопрос не отвечу. Но могу посоветовать несколько методов, которые за годы работы показали свою эффективность.

Поощрения. Я на своем веку повидал самые разные способы вознаграждения сотрудников: от упомянутой выше игрушки до подарочных сертификатов. Были и другие формы поощрения за соблюдение правил безопасности на протяжении нескольких месяцев. Конечно, если речь идет о большом коллективе, подарки могут недешево обойтись руководству. А если в качестве поощрения использовать никому не нужные безделушки, это вряд ли кого-то мотивирует. Например, мне довелось работать с компанией, которая обещала выдать подарочный сертификат на $5 за безоговорочное следование требованиям безопасности на протяжении целого квартала. Такой подарок, естественно, никого не впечатлил. Награда должна мотивировать. Конечно, я не настаиваю, что надо обещать сотрудникам телевизор с диагональю в 60 дюймов или годовую зарплату. Просто поощрение должно демонстрировать, что для вас на самом деле важны действия и отношение, которых вы добиваетесь от сотрудников.

Положительное подкрепление. В некоторых компаниях создают списки сотрудников, которые идеально соблюдали требования безопасности на протяжении X месяцев. Или списки «самых внимательных сотрудников»: в них попадают люди, на протяжении нескольких месяцев отследившие X фишинговых сообщений. В долгосрочной перспективе положительное подкрепление стимулирует желаемое поведение намного эффективнее, чем попытки пристыдить или унизить.

Дополнительное обучение. Погодите, не набрасывайтесь на меня, позвольте объяснить, что конкретно я имею в виду. Например, я неоднократно видел, какого успеха добивались компании, запускавшие программы в духе «Обучение на обеде». Они покупали пиццу или что-то подобное (если вдруг вы задумаете пригласить меня на такое мероприятие, пожалуйста, закажите зеленый салат, а то Джош будет

недоволен) и собирали сотрудников. Пока люди поедали пиццу, им показывали обучающее видео или же спикер проводил презентацию по теме, связанной с безопасностью. Конечно, многие изначально шли на такую встречу за бесплатной едой. Однако с большинства подобных мероприятий многие посетители уносили и полезную информацию. Мне доводилось бывать на таких собраниях, так что я знаю, о чем говорю. И кроме того, это еще одна отличная возможность продемонстрировать, как на самом деле для вас важны идеи и действия, которые вы хотите распространить среди сотрудников.

Воздействие «сверху». Этот метод производит почти мистический эффект, работает как заклинание. Если генеральный директор сообщит сотрудникам, что руководство компании проходит проверку фишингом раз в месяц вместе со всеми, он озвучит очень важное сообщение: «Мы все с вами в одной лодке… серьезно». Однажды я работал в компании, сотрудники которой восприняли новую программу безопасности без особого энтузиазма. Одна сотрудница неправильно отреагировала на фишинговые сообщения. Узнав, что это была проверка, она потребовала связаться со мной напрямую и 10 минут отчитывала: говорила, что я ужасный человек и мне стоило бы подумать над тем, достойное ли я выбрал дело жизни. Спустя несколько месяцев весь штат компании собрали на массовое совещание, на котором выступал в том числе и гендиректор. И вот, рассказывая о программе, он упомянул, что тоже подвергся проверке, повел себя неправильно и на собственном опыте убедился, что впредь нужно быть осторожнее. После этого ситуация в компании изменилась как по мановению волшебной палочки. Рядовые сотрудники больше не злились, агрессия по отношению к моей СИ-команде практически сошла на нет, а процент людей, соблюдавших новые требования, резко возрос. Иногда сотрудникам кажется, что руководство просто издевается над ними и пытается выставить дураками. Естественно, отношения в компании от этого не улучшаются. А вот если члены правления выражают такой инициативе поддержку действием — ситуация в корне меняется.

И еще два важных момента, о которых не стоит забывать:

- Терпение

  Не думайте, что запуск программы по обучению сотрудников возымеет мгновенный и повсеместный результат. Могут потребоваться время и серьезные усилия, чтобы персонал в конце концов проникся вашим видением проблемы.

- Управляйте ожиданиями

  Звучит знакомо? Все верно. Этот принцип работает не только с раппортом, но и в процессе создания необходимой культуры отношения к безопасности на уровне организации. Если вы сами

научились «разоблачать» фишинговые письма, не поддаваться на вишинг и видеть людей, которые пытаются проникнуть куда не следует, это не значит, что каждый сотрудник способен освоить все эти навыки с такой же скоростью.

Будьте терпеливыми и не требуйте слишком многого. Через какое-то время сотрудники окажутся на одной волне с вами.

Резюме

Хотя поначалу кажется, что это слишком сложно, поверьте мне: вы способны сформировать в своей компании культуру осведомленности в отношении вопросов безопасности. Возможно, вы оцениваете, в какой «форме» компания находится сейчас, и вам кажется, что на это уйдет слишком много времени и сил. Но дело того стоит. Польза, которую такая культура принесет компании, перевешивает все риски.

Как-то Джош прислал мне e-mail, в котором говорились: «Это путешествие на всю жизнь. Не на три месяца, не на полгода. Да, менять привычки сложно. Но ведь все мы постоянно меняемся».

Глупо повторять привычные действия в надежде получить новый результат. Допустив ошибку, старайтесь быстро двигаться дальше. Попробуйте воспользоваться советами, собранными в этой главе, но, если не добьетесь желаемого, найдите другое решение. Если метод не работает, ищите другой.

Джош постоянно трансформирует мою программу. Иногда новые требования приходят раз в неделю, но бывает, что они не меняются более месяца. Вам не обязательно менять все так же часто, но задуматься на этот счет стоит. Моя программа работает так эффективно, потому что раз в неделю я отправляю Джошу отчет о своих успехах. Он учитывает все мои перемещения, еду, активность упражнений и уровень стресса. Вся эта информация помогает ему корректировать общий курс программы. И я уверен: любое его решение основывается на детальном анализе.

Вы можете точно так же подойти к реализации программы информирования сотрудников. Для начала сформируйте подробное представление о том, что происходит в вашей организации: начиная с состояния физических объектов и заканчивая психологическими особенностями сотрудников. Постарайтесь понять, с чем связано испытываемое ими напряжение и как оно будет влиять на их решения. И когда у вас сложится полная картина, вам будет проще планировать реализацию такой программы. Продумайте траекторию развития, запустите программу и внимательно отслеживайте прогресс.

Не буду обещать, что в результате вы непременно создадите непробиваемую защиту от хакеров. Даже предполагаемый процент успеха называть не стану. Тем не менее я могу пообещать вот что:

изменения вы увидите. Постепенно вы начнете замечать, как у сотрудников формируются устойчивые представления о типах атак и способах защиты от них.

Как же применить все полученные при прочтении этой книги знания и стать пентестером, владеющим навыками социальной инженерии? Как использовать эту информацию руководству компании, которая хочет защититься от злоумышленников? Обобщающие выводы вы найдете в последней главе. И обещаю, что про Джоша в книге больше не будет ни слова (прости, Джош, твои 15 минут славы подошли к концу).

11

Что теперь?

> Ограничивать себя легко. Но если вы будете это делать постоянно, то никогда не раскроете свой истинный потенциал.
>
> Крис Уитти

Восемь-девять лет назад, начиная любимое дело, я даже не предполагал, что оно превратится в успешный бизнес и что я продолжу заниматься им в рамках некоммерческого фонда по защите детей от злоумышленников.

Случившееся за эти годы многому научило, сформировало, помогло стать тем, кем я являюсь на данный момент. Не все шло идеально, да и сейчас у меня еще есть огромные перспективы для роста. Думаю, на этом и хотелось бы сделать упор в последней главе книги.

Не существует волшебной палочки, которая превращала бы простых людей в социальных инженеров. Прочитав эту книгу, не стоит думать, будто рецепт создания идеального социального инженера прост, что стоит смешать немного раппорта, влияния, присыпать невербаликой, сдобрить доверием — и вуаля, дело сделано. Нет, это длительный процесс, требующий титанических усилий, анализа, а потом — еще больших усилий.

Ко мне постоянно обращаются с вопросами о том, как попасть в профессию, как стать настоящим социальным инженером. Ответить в двух словах не получится. Так что в этой главе я подробно расскажу о качествах, которыми просто обязан обладать профессиональный социальный инженер.

Социальные навыки[19]

Я встречал множество людей, которые отлично владели техникой и технологиями, но с работой социального инженера не справлялись: у них не получалось развиваться. В то же время мне часто попадались неуверенные в своих способностях люди, которые в итоге стали крутыми специалистами.

Я расскажу о четырех основных вещах, которые отличали этих людей. Думаю, эта информация поможет вам, если вы находитесь на этапе планирования своего профессионального развития, а возможно, даже окажется ключевой.

Скромность

Все специалисты, которым удалось преуспеть в социальной инженерии, по натуре своей скромны. И хотя смирение и мягкость принято считать проявлением слабости, я предлагаю не идти на поводу у стереотипов и задуматься. Вспомните знакомого, которого считаете по-настоящему скромным. Вспомнили? (Кстати, если называете себя — скорее всего, вы не очень правильно понимаете, о чем я тут пишу.)

А теперь, не задумываясь, ответьте: «Как я чувствую себя в обществе этого человека?» Лично я всегда ощущаю радость от того, что меня уважают, что я важен. А социальному инженеру намного полезнее вызывать у людей такие ощущения, чем считаться всезнайкой, которого даже поправить нельзя (нескромным, одним словом).

Когда мне выпала честь лично работать с Полом Экманом, я очень ясно это ощутил. Я думал, что сработаться с таким одаренным человеком будет сложно, что он окажется слишком требовательным. Но Пол показал себя очень скромным и открытым к иным точкам зрения ценителем творческой свободы. Когда меня нужно было в чем-то поправить, он действовал жестко, но при этом проявлял поразительную проницательность и умение направить в нужную сторону.

Все знакомые мне специалисты в области социальной инженерии, с которыми, кстати, было приятно работать, оказывались скромными людьми и всегда рады были выслушать конструктивную критику.

Мотивация

К работе можно относиться как к «обязаловке»: хоть это и помогает добиться поставленных целей, но тогда о своих рабочих обязанностях с радостью забываешь по окончании трудового дня. Если вы хотели найти именно такое занятие, то социальная инженерия вряд ли вам подойдет. Потому что эта профессия изменит вас — как профессионала и как личность. Причем необходимые для этого вида деятельности навыки не возникают сами по себе, а значит, чтобы сохранять конкурентоспособность, вам понадобится мотивация для роста и саморазвития.

Экстраверсия

Стоп-стоп. Прежде чем бросать книгу в шредер с криками «О нет!!! Я же интроверт!», пожалуйста, прислушайтесь ко мне: я не утверждаю, что

вам обязательно нужно меняться. Я просто считаю, что это важное для социального инженера качество и нужно научиться «включать» его на работе.

Помните, в третьей главе, посвященной профайлингу, я писал о директивном D-типе. Обычно такие люди рассказывают, что нужно делать другим, не приглашая их к обсуждению. И я часто веду себя именно так. Но чем больше я выступал и обучал других, тем больше понимал, что общение по I-типу больше подходит для преподавателя. Я решил освоить новую для себя манеру взаимодействия и «опробовал» ее на учениках. В результате я не так уставал от преподавания, а посетители еще больше полюбили мои программы.

Предлагаю вам отрабатывать один навык за раз, до тех пор пока он не превратится в удобный инструмент, который всегда под рукой и которым в любой момент можно воспользоваться. И хотя вам может не понравиться ставить перед собой задачу «заговорить сегодня с двумя незнакомцами», я очень рекомендую это делать. Со временем выполнять такие задания станет намного легче и можно будет их усложнять.

После этого вы сможете перейти к другим аспектам общения — и так до тех пор, пока не научитесь включать и выключать необходимые навыки по желанию.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Согласно исследованиям Майерс–Бриггс (https://www.myersbriggs.org/my-mbti-personality-type/mbti-basics/extraversion-or-introversion.htm?bhcp=1), экстраверты «заряжаются» в условиях социального взаимодействия, а интроверты, наоборот, теряют силы в тех же ситуациях. Экстраверты обычно общительны, свободно чувствуют себя в группе, заводят много друзей, быстро действуют, но в то же время им может не хватать внимания к деталям.

Интроверты же рефлексируют, они комфортно чувствую себя в одиночестве, имеют узкий круг общения, много времени посвящают планированию и часто долго сомневаются, прежде чем начинают действовать.

Готовность пробовать

По моим наблюдениям, боязнь ошибаться — одна из главных причин, по которым люди бросают социальную инженерию. Некоторых этот страх буквально парализует. А кто находит в себе силы для выхода из зоны комфорта, добирается до вершин успеха в СИ. Эти люди понимают, что иногда неудачи оказываются лучшим учителем. Кто готов пробовать новое, легко вливается в разные группы и быстрее адаптируется к необычным ситуациям. Я часто видел, что тяжелее всего наша работа дается тем, кто боится другой культуры, незнакомой еды и людей.

Это правда работает!

Я знаю человека, который был уверен, что из него не получится социального инженера, но освоил вышеперечисленные навыки и стал прекрасным специалистом. Помню, как он впервые появился в моей аудитории: сел в самом последнем ряду, сложил руки на коленях и опустил голову.

Я сразу понял, что передо мной чистейшей воды интроверт. Стало интересно, как его вообще занесло на мои занятия по социальной инженерии. Может, начальник заставил? Или у его компании такая политика? Занятие я начал как обычно: с доброй порции Clutch (лучшей рок-группы на земле). Едва заслышав первые аккорды, этот молодой человек, Райан, поднял глаза, и по его лицу я заметил, что ему комфортно.

«Ага, он тоже любит Clutch», — отметил я про себя. После занятий мы разговорились, и выяснилось, что ни начальник, ни политика компании не имели к приходу Райана никакого отношения. Он просто хотел бросить самому себе вызов, выйти из зоны комфорта, попробовать что-то новое — хотя прекрасно понимал, как тяжело будет это сделать.

На протяжении последующих четырех дней он с большим рвением выполнял все мои задания, и у него хватало мотивации доводить их до конца. Райан даже немного приоткрылся людям за это время, а ко мне он подходил постоянно — чтобы попросить совета или получить обратную связь по домашним заданиям.

Когда курс подошел к концу, Райан по праву получил от группы награду за самые масштабные изменения в процессе учебы. Я же во всеуслышание пообещал через год или два взять его на работу.

Однако это оказалось не так легко сделать. Райан изменился, и в компании, где он работал, это заметили. Его стали продвигать: он перешел с должности ведущего пентестера на пост начальника по социальной инженерии. Он занимался вишингом, фишингом и проникновением в разные помещения, и не просто занимался, а делал это очень эффективно.

Чтобы переманить его в свою команду на должность руководителя социально-инженерных проектов, мне понадобилось три года. Райан остался интровертом и по-прежнему любит планировать (на мой взгляд, даже слишком любит). Но он мотивирован, готов пробовать новое, учится «включать» экстраверсию и все так же не боится просить совета и помощи.

Я знаю, что однажды сам буду работать на Райана. Прямо чувствую. Так вот, если даже он преуспел в социальной инженерии — это получится и у вас. Просто применяйте четыре принципа, которые я описал выше.

Технические навыки

Один из вопросов, который мне задают чаще всего, связан с техническими знаниями, которые необходимы социальному инженеру. И тут в двух словах тоже не ответишь, но я постараюсь задать верное направление вашему поиску.

В нашей сфере деятельности без технических навыков далеко не уйдешь, ведь мы постоянно так или иначе взаимодействуем с техникой. Даже представление о том, как использовать простые технологии вроде электронных ключей, загрузочных устройств и подключения к VPN, может существенным образом помочь вам в процессе разработки легенды и получения необходимого доступа.

Нужно ли при этом быть экспертом в создании эксплойтов? Вовсе не обязательно. Чтобы понять, насколько технологически подкованным должен быть социальный инженер, я использую следующее правило. Вы будете работать самостоятельно или в команде? Если самостоятельно, то без технических навыков вам не обойтись: любые ваши ограничения будут сужать спектр услуг, предлагаемых вами клиентам.

Если же вы собираетесь работать в команде, то ориентироваться нужно на наличие навыков у других ее членов: в отличие от одиночной работы, вы сможете позволить себе некоторые послабления. В моей команде работают прекрасные специалисты как технического, так и нетехнического профиля.

Если вы считаете, что технические навыки вам необходимо развивать, то рекомендую обратить внимание на следующие сферы:

- базовые знания о компьютерах;
- базовые знания об офисных программах (в частности, Word и Excel);
- знания о том, из каких элементов состоит компьютер и как эти элементы функционируют;
- умение работать в операционных системах Mac, Windows и Linux;
- понимание механизмов работы Сети;
- умение настраивать почтовый сервер;
- навыки фоторедактирования.

Если вы планируете использовать в пентестах эксплойты, вам также пригодятся:

- знания о платформах вроде Metasploit и Empire;
- умение читать и понимать код;
- умение писать код.

Образование

«Какое образование нужно иметь, чтобы стать социальным инженером?» — каждый раз, когда мне задают этот вопрос (а происходит это намного чаще, чем можно себе представить), я отвечаю, что не считаю себя достаточно квалифицированным специалистом, чтобы советовать что-то конкретное. В конце концов, в свое время я расстался с колледжем после того, как написал программу, осуществлявшую автоматическое сканирование списка телефонных номеров и звонки на них. Тогда декан вместе с полицейскими «предложили» мне закончить обучение как можно скорее.

ЗАБАВНЫЙ ФАКТ

В начале 1990-х еще не были разработаны законы о компьютерных правонарушениях, и «хакерами» называли просто интересующихся энтузиастов, а не злоумышленников, стремящихся что-то разрушить. Я написал программу, которая работала так. Она связывала последовательно два телефонных модема, затем набирала номер и отправляла несколько цифр, которые отключали номер на пять минут, после чего обрывала соединение. Затем эти действия повторялись снова. Я использовал так называемую поточную обработку, позволявшую программе одновременно набирать огромное количество номеров. Этот скрипт на целый день вырубил 60% телефонных систем штата. После чего меня и «попросили» покинуть альма-матер.

И хотя образовательная база у меня весьма сомнительная, хочу высказать несколько соображений о том, какое образование будет полезным для будущего социального инженера. Речь пойдет не о магистерской степени, но скорее о некоторых базовых знаниях в следующих сферах:

Психология. Не только психологам и психотерапевтам важно знать, как люди принимают решения. Социальным инженерам это тоже пригодится.

Устная и письменная речь, грамотность. Вы можете быть лучшим социальным инженером на земле, но, если вы при этом не способны сформулировать четкий и понятный отчет, ваши заслуги едва ли кто-то признает. Я рекомендую пройти качественные курсы по развитию языковых навыков и обогащению профессионального словаря.

Социальная психология. Понимание того, как люди взаимодействуют в социальных группах и какое влияние группы оказывают на них, обязательно поможет вам в работе.

Возможно, вы сейчас удивитесь: неужели этого достаточно? Но я ведь говорил, что не претендую на статус гуру из мира высшего образования. Просто советую, исходя из собственного опыта. Только, пожалуйста, не думайте, что без формального образования в перечисленных сферах вам заказан путь в мир социальной инженерии. Вы можете читать книги, изучать сайты, слушать подкасты и общаться с более опытными людьми. Этого бывает достаточно, чтобы сформировать необходимую базу знаний.

Нам необязательно становиться психологами, психотерапевтами, лингвистами и социальными психологами. Просто нужно понимать, какие принципы задействованы в происходящем и как именно они работают.

Профессиональные перспективы

Если бы я мог описать в этой книге безотказный метод поиска заказчиков, думаю, она сразу же после публикации получила бы статус бестселлера по версии The New York Times. Но, к моему великому сожалению, такого метода просто не существует. Тем не менее я могу подсказать, какие пути в принципе можно рассматривать.

Открыть свою компанию

Вы можете начать продавать СИ-услуги организациям в вашем регионе. Сегодня открывать подобные компании проще, чем во времена, когда я только начинал (и не благодарите).

В самом начале своего профессионального пути я предлагал бесплатно отправить пять (да, всего пять) фишинговых писем, чтобы потенциальные заказчики прониклись моей идеей. И все равно получал много отказов. Сегодня же люди сами просят использовать СИ в ходе пентестов. Во многом такой сдвиг произошел благодаря публикациям в СМИ, где освещались потенциальные угрозы, связанные с социальной инженерией. Так что вам будет легче начинать.

Но даже несмотря на изменения, произошедшие за последние несколько лет, на пути социального инженера до сих пор встречается множество преград. Просто поставьте себя на место заказчика, которого вы просите: «Дайте мне список пользователей вашей сети, а я подвергну их фишингу и вишингу. Ах да, и еще мне хотелось бы проникнуть в ваш офис и что-нибудь оттуда унести. И раз уж пришел, могу заодно установить программу для получения удаленного доступа к вашей системе и хакнуть ее».

Прежде чем заказывать такие услуги, большинство компаний захочет узнать побольше об исполнителе, в частности ознакомиться с отзывами об уже завершенных проектах. Понятное дело, в начале пути с этим могут возникнуть определенные трудности. Но это не повод погружаться в отчаяние и плакать, забившись в угол. Существуют способы формирования хорошей репутации.

Выступите на конференции, заведите и раскрутите блог, чтобы вас читали и комментировали. Если ваше имя станет известным даже в узких кругах, вам будет легче доказать потенциальным заказчикам, что вы — достойный претендент для оказания необходимых им услуг. Я несколько раз наблюдал, как люди, не имеющие практического опыта в социальной инженерии, открывали таким образом успешный бизнес. Они

приходили на DEF CON и участвовали в игре «Захват флага» для социальных инженеров (SECTF), где показывали отличный результат или даже побеждали, после чего открывали компании, предлагающие СИ-услуги. Формирование кредита доверия помогает развиваться.

Устроиться в компанию, занимающуюся пентестингом

Большинство компаний, занимающихся пентестингом, предлагают СИ-услуги в том или ином виде. И я видел, как некоторые молодые специалисты находили себе работу через них. Если вы только закончили учиться и еще не набрали никакого опыта, возможно, имеет смысл начать с самого низа.

Впрочем, устроившись на работу, обязательно подчеркните, что хотели бы заниматься вишингом, созданием легенд и т.п. Чем лучше вы будете справляться с поставленными задачами, тем больше новых возможностей даст вам руководство. При благоприятном стечении обстоятельств вы имеете все шансы быстро продвинуться по карьерной лестнице социальной инженерии.

Нужно понимать, что такой путь может занять месяцы, а то и годы. Бывает, что сотрудник проявляет инициативу, но компании этого не нужно. В таком случае решите для себя, как долго вы готовы продолжать попытки.

Если вы выберете этот путь, рекомендую запастись терпением и решимостью по отношению к освоению новых навыков, необходимых для развития в штате компании и постепенного выхода в самостоятельное плавание.

Устроиться в компанию, занимающуюся социальной инженерией

Несколько минут в Google-поиске — и вот передо мной уже целый список компаний, занимающихся социальной инженерией; некоторые даже предлагают исключительно СИ-услуги. Например, моя компания занимается только этим, и мы каждый месяц получаем большое количество заявок от людей, которые хотели бы у нас работать. Я бы с удовольствием нанял всех (кто подходит по уровню квалификации), но мы набираем новых сотрудников, только когда появляются вакансии (логично, да?).

Тем не менее отсутствие анонсированных вакансий не должно вас останавливать: все равно дайте понять интересующим вас компаниям, что готовы работать. Укажите, о чем вы писали, рассказывали, в каких проектах уже участвовали. Скажите, что хотели бы попасть на собеседование, когда откроется вакансия. Путь к работе мечты может

начаться для вас с попадания в список претендентов на место в такой компании.

Какой бы путь вы ни выбрали, помните: новые люди в этой сфере очень нужны. Социальная инженерия в ближайшее время не перестанет быть актуальной. И потребность в квалифицированных и небезразличных специалистах тоже не исчезнет.

Будущее социальной инженерии

Давайте на секундочку переключимся на серьезный тон. Ведь социальную инженерию используют не только хакеры (подробнее об этом можно почитать в отчетах DBIR, CISCO и др.), но и намного более опасные злоумышленники.

Каждый день появляются новости о том, как люди уходят из дома, бросают семьи и вступают в террористические организации. Как это происходит?

Если вы проанализируете эти печальные истории, то наверняка увидите в них приемы социальной инженерии, упомянутые в этой книге. Люди, вступающие в ряды террористов, обычно испытывают сильные эмоции, злятся, ищут свое «племя». И когда находят его, получают ответы на свои вопросы и «решения» своих проблем. Люди чувствуют себя нужными, желанными, принятыми. Поначалу новое «племя» не просит от них ничего серьезного: в этот период выстраивается связь и устанавливается доверие. Но это лишь до тех пор, пока не закончится процесс обращения.

В статье Ричарда Флорида под названием «География иностранных бойцов ИГИЛ[20]» (CityLab, август 2016, https://www.citylab.com/equity/2016/08/foreign-fighters-isis/493622/) сказано, что порядка 19 000 людей из Туниса, России, Саудовской Аравии, Турции и Иордании бросили свои семьи и вступили в ИГИЛ. В западных странах показатели ниже (не больше 2000 человек из Великобритании, Франции, Германии, США и др.), но принципы рекрутинга используются те же.

Еще одна тревожная тенденция: принципы социальной инженерии используют преступники, совращающие детей. Они завязывают с детьми отношения в онлайн-чатах, внедряясь в их «племя». Такие хищники отыскивают детей, у которых плохие отношения с родителями или тяжелая атмосфера дома, устанавливают с ними раппорт, активно слушают, задают открытые вопросы, а потом внедряют в детские головы удобные для себя идеи и представления.

Согласно отчету Национального центра поиска пропавших и эксплуатируемых детей (NCMEC), в 2017 году в США пропавшими без вести числились 465 676 детей (http://www.missingkids.com/footer/media/keyfacts). За тот же временной

промежуток, по данным ФБР на основе анализа 25 000 случаев побегов из дома, каждый седьмой ребенок становился жертвой секс-торговли. И огромное количество детей оказывались в руках педофилов.

Да, это очень больная тема. Но я хочу доказать вам, что сегодня изучение социальной инженерии не теряет актуальности. Воздействию злоумышленников подвергаются компании, доверчивые старики и дети, жертвы террористической пропаганды. Принципы СИ используются активно, они очень востребованны.

Миру нужны люди, умеющие применять эти принципы в благих целях: чтобы защищать, информировать и вооружать простых людей знаниями и навыками, позволяющими противостоять подобным атакам. Это нелегкий путь. Но поверьте мне, дело того стоит.

За последние восемь лет мне довелось поработать с десятками компаний со всего мира. Я своими глазами видел, как резко снижалась после этого их уязвимость к СИ-атакам. Например, в одной компании количество вредоносного кода, выявляемого в корпоративной сети, снизилось на 87%. Руководство компании напрямую связывало эти результаты с нашей деятельностью по просвещению сотрудников в вопросах фишинга.

В отчете другой компании говорилось, что благодаря работе с нами их сотрудники научились выявлять, пресекать и сообщать об активных фишинговых атаках.

Один из учеников рассказал, что посещение моего пятидневного курса спасло его брак. Хотя я никогда не позиционировал курс как практику семейной психотерапии, но, конечно, порадовался, что переданные мною знания об общении, раппорте и влиянии помогли ему дома и в личных отношениях.

Кроме того, я принимал участие в спасении детей — как через свою компанию, так и через фонд «Невинные жизни» (https://www.innocentlivesfoundation.org/). Те самые навыки, которым я каждый день обучаю, помогают находить хищников, охотящихся на наших детей. И это очень благодарный труд.

Наконец, последний, и очень личный, аргумент. Мне удалось научить этим навыкам своих детей. Они растут с пониманием своей сущности, они менее уязвимы к подобным атакам и (по моему, не такому уж и скромному, мнению) являются одними из самых гармоничных и удивительных людей, которых я знаю.

Изучение собранных в этой книге навыков приносит пользу не только в профессиональной, но и в повседневной жизни. Я надеюсь, что моя книга вдохновит вас продолжать учиться. Надеюсь, вы почерпнули из нее несколько полезных идей. Ну а если вы скептик или энтузиаст, надеюсь, книга дала вам поводы для увлекательных размышлений.

Я буду очень рад, если вы поделитесь своим мнением о книге и внесете свой вклад в развитие знаний о социальной инженерии. Призываю вас использовать описанные навыки каждый день. И желаю вам безопасности и защищенности.

[1] Allen W. Dulles. Memorandum Respecting Section 202 (Central Intelligence Agency) of the Bill to Provide for a National Defense Establishment, April 25, 1947, p. 525.

[2] Donna O'Harren, "Opportunity Knocking: Open Source Intelligence For the War on Terrorism," Thesis, Naval Postgraduate School, December 2006, p. 9.

[3] Крупные конференции хакеров и специалистов по информационной безопасности. DEF CON проводится в Лас-Вегасе с 1993 года, DerbyCon — с 2011 года в Луисвилле. — Прим. науч. ред.

[4] «Захват флага» (Capture the Flag) — командная игра, участники которой стремятся захватить «флаг» соперника. В разных вариантах игры «флагом» может быть что угодно: настоящий флаг, предмет или информация. В книге речь идет об игре для специалистов по информационной безопасности, в которой игроки либо выполняют задания по взлому защиты, либо охраняют свои серверы, атакуя при этом серверы противников. «Флагом» здесь становится информация, которую надо выкрасть у других и защитить у себя. Сайт игры в России: https://ctfnews.ru. — Прим. науч. ред.

[5] От англ. voice + phishing — голосовой фишинг. Выведывание частной информации в телефонном разговоре. Как правило, социальный инженер выдает себя за того, кому жертва вишинга привычно доверяет. Примером вишинга может быть телефонный звонок, в котором мошенник представляется сотрудником службы безопасности банка. Он якобы пытается предотвратить хищение средств с карты жертвы и, пользуясь незнанием обычного человека, склоняет его выдать данные для доступа к удаленному управлению счетом.

[6] Фишинг. От англ. fishing — «рыбная ловля». Выведывание частной информации с помощью подкладывания пользователю ложного интернет-сайта, внешне неотличимого от того, которым он пользуется. Вводя логин и пароль к ресурсу на поддельном сайте, пользователь передает мошенникам доступ к ресурсу с частной информацией, банковскому счету и т.д. Как правило, при фишинге используют массовую рассылку писем, надеясь, что хотя бы немногие из получивших письма клюнут на поддельный сайт. — Прим. науч. ред.

[7] Используемой в профессиональном жаргоне кальке с английского «претекст» мы предпочли более употребительное слово «легенда». — Прим. науч. ред.

[8] Имперсонация. От англ. impersonation — перевоплощение. Выдача себя за другого человека, подделка чужого профиля в социальной сети

для получения информации, нанесения ущерба репутации или шантажа. Например, подделка сайта органа власти или учетной записи известного человека. — Прим. науч. ред.

[9] В текстах по системной инженерии распространен также термин OSINT — Open Source Intelligence. Между профессиональным жаргоном и сочетанием, понятным широкой аудитории, мы выбрали последнее. — Прим. науч. ред.

[10] Фрейминг. От англ. frame — рамка. Зависимость восприятия ситуации от ее контекста. Изменяя форму подачи информации (по-разному задавая рамки), можно управлять контекстом и через него влиять на ее восприятие. Например, распространена манипуляция с помощью перевода фрейма с рабочего на личный. Начальник говорит подчиненному, что он недоволен его работой. Подчиненный смещает фрейм на личный: «Вы всегда придираетесь ко мне, потому что я вам не нравлюсь». Если начальник поведется на манипуляцию и примет предложенный фрейм, дальнейшая дискуссия пойдет в русло личных пристрастий, а значит, собственно промах подчиненного будет забыт. — Прим. науч. ред.

[11] Пентест. От англ. penetration + test — тестирование на проникновение. Метод проверки безопасности офиса или закрытой территории, в котором моделируется попытка проникновения людей на охраняемый объект. Этот же термин используют для анализа уязвимостей информационной системы: эксперимент с попыткой ее взлома. — Прим. науч. ред.

[12] Распознавание лжи. — Прим. науч. ред.

[13] Спуфинг — от англ. spoofing, подмена. Ситуация, в которой устройство, программа или человек представляются чем-то или кем-то другим с помощью ложного идентификатора. Например, мошенник во время телефонного вызова подставляет знакомый пользователю номер телефона банка. — Прим. науч. ред.

[14] От англ. «нефтененавистник».

[15] Признание и принятие своих или чужих мыслей, эмоций, чувств и поступков как понятных. — Прим. ред.

[16] Согласно исследованиям Пола Экмана, человек в целом способен контролировать мимику и скрывать проявления эмоций, однако на короткое мгновение, до 1/5 секунды, эмоции все же отражаются на лице. Быстрые непроизвольные проявления эмоций Экман назвал микровыражениями. Хотя в большинстве случаев человеку удается скрыть эмоции, тренированный взгляд специалиста способен различать их, что может использоваться, например, для распознавания лжи. — Прим. науч. ред.

[17] В РФ законодательно ограничен оборот техники для скрытого наблюдения. Наказание за него предусмотрено ст. 138.1 УК России

«Незаконный оборот специальных технических средств, предназначенных для негласного получения информации». — Прим. науч. ред.

[18] Fisher — «рыбак» (англ.).

[19] Soft skills (англ. «мягкие» навыки) — универсальные компетенции, не поддающиеся количественному измерению: пунктуальность, коммуникабельность, креативность, умение работать в команде и т.п. Зависят от характера человека и приобретаются с личным опытом. — Прим. ред.

[20] Запрещенная в России организация.

Переводчик Анастасия Соломина

Научный редактор Денис Букин

Редакторы Ирина Беличева, Елена Аверина

Главный редактор С. Турко

Руководитель проекта О. Равданис

Корректоры Е. Чудинова, С. Чупахина

Компьютерная верстка А. Абрамов

Дизайн обложки Ю. Буга

© 2018 by John Wiley & Sons, Inc., Indianapolis, Indiana

All rights reserved. This translation published under license with the original publisher John Wiley & Sons, Inc.

© Издание на русском языке, перевод, оформление. ООО «Альпина Паблишер», 2020

© Электронное издание. ООО «Альпина Диджитал», 2020

Хэднеги К.

Искусство обмана: Социальная инженерия в мошеннических схемах / Кристофер Хэднеги; Пер. с англ. — М.: Альпина Паблишер, 2020.

ISBN 978-5-9614-3102-5