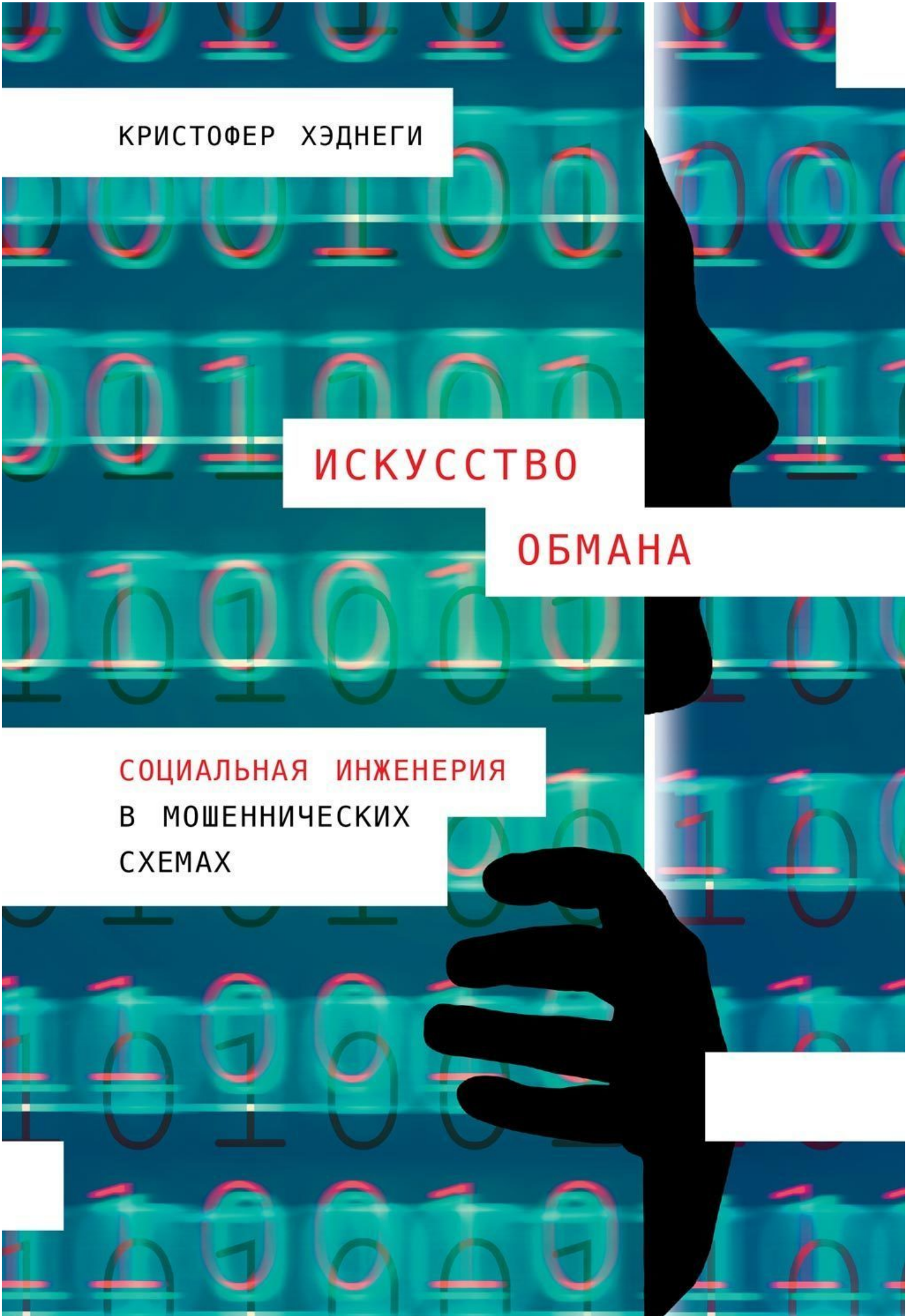
КРИСТОФЕР ХЭДНЕГИ
ИСКУССТВО
ОБМАНА
СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ
В МОШЕННИЧЕСКИХ
СХЕМАХ

Кристофер Хэднеги

Искусство обмана

«Альпина Диджитал»

2018

Хэднеги К.

Искусство обмана / К. Хэднеги — «Альпина Диджитал», 2018

ISBN 978-5-9614-3102-5

Бывало ли так, что вам звонил человек и представлялся сотрудником банка? Или приходило письмо со ссылкой, по которой вы, к счастью, не перешли? Технологии, при помощи которых злоумышленники пытаются получить доступ к вашим паролям или данным, основаны на социальной инженерии – науке об изощренном и агрессивном манипулировании поведением людей. Она использует целый арсенал инструментов: давление на жалость, умение запудрить мозги или вывести из себя, проявить несвойственную жадность и поставить в неловкое положение, вызвать чувство вины или стыда и многое другое. Становясь жертвами обмана, мы не только подвергаемся риску сами, но и можем сильно подвести своих коллег и близких. Кристофер Хэднеги, всемирно известный специалист по социальной инженерии, научит вас распознавать манипуляции всех типов и противодействовать мошенникам всех мастей. Больше никто не сможет заставить вас сделать то, что вы делать не планировали, – расстаться с деньгами, выдать важную информацию, совершить опасные действия. Все примеры, которые приводит Хэднеги, взяты из его личной и профессиональной практики.

ISBN 978-5-9614-3102-5

Содержание

Кристофер Хэднеги
Искусство обмана: Социальная инженерия в мошеннических схемах

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*

* * *

Всем, что случилось в моей жизни социального инженера, отца, мужа, начальника, друга, я обязан своей прекрасной жене. Ариса, мою любовь к тебе не выразить словами.

Колин, сынок, я наблюдаю, как ты растешь и становишься молодым мужчиной, которого не проведешь. Когда мы вместе работаем, я понимаю, что это не зря. Я тебя люблю.

Амайя, свет моей жизни! Ты знаешь, как заставить меня улыбнуться даже в самый мрачный день, ты – радость моего сердца и моя любовь. Нет слов, чтобы выразить мою гордость за то, каким хорошим человеком ты становишься.

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.

---

[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.

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.

[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*.

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 Оберн-ском 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 Фелоном 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

---

[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.*

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

[7] Используемой в профессиональном жаргоне кальке с английского «претекст» мы предпочли более употребительное слово «легенда». – *Прим. науч. ред.*

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,

[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.*

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.

[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.*

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.

---

[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.*

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.

Конец ознакомительного фрагмента.