

# РАЗДЕЛ «СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ»

*Какой взлом обходится без социальной инженерии? Социотехнический взлом в наше время стал совершенно обычным делом. В этом разделе мы обучим тебя социальной инженерии и ее тонкостям, научим ее применять. Расскажем о техниках, которые идут в ход, и о разнообразных тонкостях, которых в деле хакера — великое множество.*

Социальная инженерия, иногда называемая наукой и искусством взлома человеческого сознания, становится все более популярной в связи с повышением роли социальных сетей, электронной почты или других видов онлайн-коммуникации в нашей жизни. В сфере информационной безопасности данный термин широко используется для обозначения ряда техник, используемых киберпреступниками. Последние имеют своей целью выманивание конфиденциальной информации у жертв либо побуждают жертв к совершению действий, направленных на проникновение в систему в обход системы безопасности.

Даже сегодня, когда на рынке доступно огромное количество продуктов для обеспечения информационной безопасности, человек все еще владеет ключами от всех дверей. Будь то комбинация учетных данных (логин и пароль), номер кредитной карты или данные для доступа к онлайн-банку, самое слабое звено в системе обеспечения безопасности — это не технологии, а живые люди. Таким образом, если злоумышленники применяют к пользователям манипулятивные психологические техники, очень важно знать, какие приемы наиболее характерны в данной ситуации, а также понимать принцип их работы, чтобы избежать неприятностей.

Социальная инженерия — понятие совсем не новое, оно появилось давным-давно. Известными специалистами-практиками в этой науке стали, например, Кевин Митник и Фрэнк Абаньяле, которые на сегодняшний день являются ведущими консультантами по безопасности. Они живая иллюстрация того, что преступники могут превращаться в уважаемых экспертов. К примеру, тот же Фрэнк Абаньяле был одним из самых знаменитых и виртуозных мошенников: он умел создавать множество личностей, подделывать чеки и обманывать людей, вытягивая из них конфиденциальную информацию, необходимую для работы мошеннических схем. Если вы смотрели фильм «Поймай меня, если сможешь», вы имеете представление о том, на что способен специалист по социнженерии, если он имеет перед собой ясную цель. Вам просто следует помнить, что для получения от вас нужной информации социнженер может использовать

различные мошеннические схемы, не ограничивающиеся приемами, связанными с технологиями или компьютерами, так что лучше пользователям с осторожностью относиться к подозрительным действиям, даже если они кажутся обычными. Классическим приемом, например, является выманивание пароля в телефонном звонке. Кажется, что никто в здравом уме не сообщит свой пароль постороннему, но звонок «с работы» в 9 утра в воскресенье, требующий приехать для какой-то мелочевой технической операции над вашим компьютером, несколько меняет дело. Когда «ваш администратор» предложит просто сказать ему пароль, чтобы он все сделал за вас, вы не только сообщите пароль, но и поблагодарите его за заботу! Ну, может, не лично вы, но примерно половина ваших коллег поступит так гарантированно.

Большинство киберпреступников не станут тратить время на осуществление технологически сложных приемов взлома, если необходимые сведения можно получить, используя навыки в области социнженерии. Более того, существует множество сайтов, где описаны принципы работы подобных техник и причины их успеха. Один из этих сайтов называется [SocialEngineer.org](https://social-engineer.org), и он предлагает весьма полезную основу для теоретического изучения принципов социнженерии, дополняя ее большим количеством реальных примеров.

Мы используем речь каждый день, влияя на действия друг друга, хотя часто не замечаем этого. Но язык с точки зрения социнженерии имеет несколько недостатков, так как он связан с нашим субъективным восприятием фактов, при котором мы можем опустить некоторые части истории, исказить смысл или сделать некоторые обобщения. НЛП, или нейролингвистическое программирование, которое изначально было создано для лечебных целей, сегодня считается «мутировавшей» формой гипноза, используемой социнженерами как инструмент манипуляции жертвами и оказания на них влияния с целью побудить их выполнить действия, ведущие к успеху атаки. В результате данной тактики жертва может сообщить свой пароль, разгласить конфиденциальную информацию, отказаться от какой-либо меры обеспечения безопасности, то есть, может сделать все что угодно, чтобы убрать препятствия на пути злоумышленников.

Хотя связь между психологией и хакингом кажется чересчур натянутой, на самом деле онлайн-атаки основаны на тех же принципах, которые лежат в основе «офлайнового» мошенничества. Принцип возвратности («если я окажу тебе услугу, ты окажешь услугу мне»), принцип социальной проверки (вы оцениваете свое поведение как правильное, если наблюдаете такое же поведение у большинства), преклонение перед авторитетами (проявление большей степени доверия к сотруднику полиции, врачу, сотруднику технической поддержки, кому-либо более «высокого ранга») — это универсальные для всех способы выстраивания общения в социуме и

удовлетворения наших базовых социальных инстинктов. Социнженер знает, на какие кнопки нажимать, чтобы получить желаемый ответ, создавая контекст (канву) для формирования правдоподобной легенды, которая смогла бы создать ощущение срочности. Для опытных специалистов в сфере социнженерии не составит труда обойти рациональное мышление человека, и им понадобится только доля секунды, чтобы добиться преимущества и получить от жертвы необходимые данные.

Однако в данной статье мы в большей степени обратим внимание на различные техники, используемые онлайн-мошенниками для незаконного получения информации и прибыли от жертв, которые «хотели как лучше». Как мы уже упомянули, принципы, используемые для мошеннических схем в Интернете, похожи на те, которые используются в реальной жизни, но так как Интернет — это огромная машина распространения информации, одно фишинговое сообщение может быть отправлено миллионам получателей в течение самого короткого времени. То есть в таких условиях данный тип атак может превратиться в беспроигрышную лотерею: даже если только небольшая часть от общего числа потенциальных жертв попадется на удочку, это все равно означает огромную прибыль для организации или человека, стоящего за атакой.

Сегодня одним из самых распространенных методов получения конфиденциальной информации является фишинг (термин образован от игры слов password harvesting fishing — «ловля паролей»). Фишинг можно охарактеризовать как тип компьютерного мошенничества, который использует принципы социальной инженерии с целью получения от жертвы конфиденциальной информации. Киберпреступники обычно осуществляют свои действия при помощи электронной почты, сервисов мгновенных сообщений или SMS, посылая фишинговое сообщение, в котором напрямую просят пользователя предоставить информацию (путем ввода учетных данных в поля сайта-подделки, скачивания вредоносного ПО при нажатии ссылки и т.д.), благодаря чему злоумышленники получают желаемое при полном неведении со стороны жертвы.

Мы наблюдали процесс развития вредоносного ПО, который во многом использовал принципы социнженерии. Раньше факт заражения компьютера вирусом был весьма очевиден: пользователь видел странные сообщения, иконки, картинки — одним словом, все, что обнаруживало участие злоумышленника. Сегодня нас уже не удивляют примеры вредоносного ПО, которое получает доступ к системам жертв путем применения трюков, характерных для социнженерии, и остается невидимым для пользователя до того момента, как выполнит свою задачу. Бесконечная игра в кошки-мышки между хакерами и компаниями, создающими средства информационной безопасности, подтверждает: образование и информирование — это ключевой защитный механизм, необходимый для пользователей. Они

должны следить за новостями и новыми веяниями в мире информационной безопасности, а также знать о ключевых тактиках мошенников.

Множество интересных примеров взлома основаны на техниках социнженерии, которые, в свою очередь, помогают злоумышленникам доставить вредоносное ПО жертвам. Среди наиболее популярных — фальшивые обновления Flash Player и других популярных программ, вшитые в документ Word исполняемые файлы и многое другое.

Большинство описанных выше методов проведения атаки направлены на жителей Латинской Америки, так как технологические угрозы такого типа не до конца понятны или распространены в регионе, а если еще и принять во внимание, что большинство компьютеров работают с устаревшим ПО, это дает киберпреступникам отличную возможность заработать. Только недавно некоторые банки усилили меры обеспечения информационной безопасности для пользователей онлайн-банкинга, но до сих пор множество уязвимостей в системе безопасности способствуют успеху тактик социнженерии. Интересно, что многие особенности этого региона перекликаются с российскими, поэтому киберпреступники СНГ и Латинской Америки весьма активно обмениваются опытом и перенимают друг у друга удачные находки. Популярны другие типы атак, которые даже не всегда попадают в категорию компьютерного мошенничества. Схема, известная как «виртуальное похищение», использует практики социнженерии, а в качестве средства связи выступает телефон. Злоумышленники обычно звонят жертве и говорят, что член семьи был похищен и для его освобождения требуется незамедлительно заплатить выкуп. Преступник создает ощущение срочности и страха, жертва выполняет требования мошенника, даже не убедившись, на самом ли деле похищен кто-то из родственников. Похожая схема популярна при атаках на пожилых людей и может быть названа «виртуальной болезнью» — когда жертве звонят якобы из поликлиники, говорят, что в недавних анализах есть признаки опасного заболевания и нужно незамедлительно лечь на операцию для спасения жизни, разумеется, платную. После оплаты, конечно, никого не оперируют, потому что болезни никакой и не было.

***Давайте продолжим нашу лекцию интереснейшими примерами социальной инженерии. Они наверняка вас удивят и дадут идеи и понимание.***

## **«Взлом QIWI»**

Способов заработка в интернете довольно много, но все они либо неэффективные, либо же «черные». Мы никогда не приветствуем злодеяния и кражу у честных людей. Однако, в деньгах заинтересованы. Обчистить мошенника в интернете казалось не таким уж и черным делом.

Во времена рассвета синтетических наркотиков открывались целые форумы по продаже и закупке наркотических средств. Дилеры нуждались в особой защите, но их каналы были не такими уж и защищенными. Как правило, общение с клиентами проводилось через уязвимые мессенджеры вроде skype, jabber и старой доброй icq. Оплату дилеры принимали в основном на самые популярные платежные системы, но в основном на Киви-кошелек по номеру телефона. На балансе таких кошельках находились и находятся огромные деньги. Получить доступ к кошельку Киви -означает получить эти самые деньги. Наркодилеры не принимают никаких файлов, не переходят по внешним ссылкам, стараются не вступать в тесный контакт с клиентом. Все, что мы имеем, это номер кошелька Киви.

### **Доверенность**

Техническая поддержка Киви скептически относилась к восстановлению доступа к кошельку. Если вы потеряли доступ, то восстановить пароль можете только если сим карта у вас на руках. Тогда мы и стали думать, как получить себе дубликат сим-карты. Первым шагом, мы звонили оператору сотовой связи и пытались каким-либо образом переадресовать смс-сообщения и звонки на свой номер, что окончилось неудачей. Но мы выяснили, что на основе генеральной доверенности, все-таки, можно получить дубликат сим-карты. Однако этот способ был очень опасным и сложным.

Суть состояла в том, чтобы пробить паспортные данные человека, зарегистрированного на сим-карту. Затем найти человека, на кого можно будет оформить генеральную доверенность. После чего этот человек должен будет прийти в отделение сотовой связи и получить сим-карту. Но для составления генеральной доверенности нужен еще и второй человек, которому принадлежит сим-карта, поэтому идея показалась напрасной. Однако, мы все же решили проверить на себе. У моего знакомого была генеральная доверенность на своего родственника. Мы пришли в отдел и были поражены тем, что операторы никак не проверяли данную доверенность на наличие в реестре, а, значит, можно указать совершенно несуществующего нотариуса и нарисовать любую печать. Грубо говоря, документ можно полностью подделать без участия жертвы.

На хакерских форумах были люди, активно предлагающие свои услуги по пробиву\* информации о любом мобильном номере. Стоимость была сравнительно низкая, поэтому мы и воспользовались этим. Получив номер кошелька для оплаты наркотических средств от дилера, мы передали его пробивале\*\*. По сути, это те же операторы в мобильных офисах. Через час получили паспортные данные этого номера. Взяли за основу шаблон генеральной доверенности, ранее использованной моим знакомым. Переписали данные, переделали печать и ФИО нотариуса. Поставили другую подпись и все готово. Придя в офис к оператору, было весьма тревожно, но действовали, не подавая виду. Покрутив свежую напечатанную доверенность в руках, оператор без лишних вопросов оформил на новые паспортные данные сим-карту и выдал нам в руки в течение 5 минут. Слишком уж просто. Мы сразу же отправили код восстановления пароля на сайте киви и восстановили пароль за минуту. Работали мы так очень долго и это приносило огромные деньги.

Однажды операторы заподозрили частые посещения в офис и решили проверить доверенность. Все обошлось и нам удалось уйти. По этой схеме можно работать, если соблюдать особые меры предосторожности. Во-первых, необходимо было посещать разные офисы с периодичностью примерно 1-2 раза в неделю. Во-вторых, люди должны постоянно меняться. Причину, по которой мы восстанавливали сим-карты, операторы не спрашивали. Их мало волновал и сам документ. Они даже не делали скан-копию. Все эти ошибки были результатом безответственного отношения работников офисов.

*\* проверить или узнать информацию о ком-либо, чём-либо*

*\*\* лицо, предоставляющее услуги по пробиву*

## **Подмена**

Скажу честно, до такого было не так трудно додуматься. Труднее было это реализовать. И так, почти все платежные средства, а также мобильные операторы, предоставляют возможность использовать USSD запросы. На сайте киви такие команды тоже были. Объясню доступным языком. Предположим, у вас есть киви-кошелек, на котором активирована функция USSD. Активируется она в настройках кошелька и, как правило, включена автоматически. Если сим-карта находится у вас в телефоне, то вы можете совершить перевод средств простой смс командой «перевод 89123456789 1000» на номер 7494. С вашего счета спишут 1000 рублей и переведут на счет другого киви кошелька с номером 89123456789. Возникает мысль, а что, если

подделать номер отправителя и, скажем, не имея под рукой сим-карты жертвы, отправить смс с переводом средств на свой кошелек. Сервисы по отправке смс с подменой отправителя существовали и активно работали, причем многие из них совершенно бесплатно. Предназначены они были скорее для розыгрышей, но мы используем их для своих целей. Проблема была в том, что подделывать запросы на короткие номера было невозможно! Тут возникает другой вопрос, а ведь короткий номер к чему-то должен привязываться? И да, действительно, у каждого короткого номера есть федеральный. И мне удалось его найти. Точнее был даже не один номер, а целая корпоративная группа. Номер был оформлен на компанию ООО «Бифри», использовался тариф «мобильное информирование», баланс на номере минус 400 тысяч рублей. Главное, что если отправить на этот номер смс, то автоматически переадресуется на короткий 7494. То, что нужно!

Приступаем к атаке. Находим рабочий сервис с подменой смс отправителя. Указываем отправителем номер нашей жертвы, номер получателя – федеральный номер Киви, а в теле письма пишем следующую команду: «перевод 89123456789 1000», где 89123456789 – номер нашего Киви. Отправляем смс и со счета жертвы снимается 1000 рублей и переводится на наш номер – 89123456789. Максимально можно было переводить по 5000 рублей. Поэтому приходилось совершать сразу несколько команд, если на кошельке была большая сумма. Пир был не долгим. Киви изменила систему ussd, добавив подтверждение по смс. К тому же, операторы сотовой связи запретили подменять смс через сторонние шлюзы. Кое-какие сервисы все же работали, но это уже не имело значения.

## «Сломай барыгу»

*Я не помню, когда интернет так широко монетизировали. Все чаще люди стараются уйти в онлайн работу в поисках различных способов заработка. Форумы о заработке предлагают такие схемы, как «белые», так и «черные». Конечно, можно долго спорить о том, что все белые схемы – бесполезны, так как никто бы не стал делиться идеями бизнеса, который якобы приносит миллионы, а цена этой идеи составляет жалкие 5 тысяч деревянных. Поэтому самые яркие примеры заработка можно наблюдать именно в «черных» схемах. Сюда можно отнести: кардинг, хакинг, фрод, ддос, вымогательство, торговля незаконными вещами и препаратами, и многое другое. Во-первых, это реально приносит прибыль. Во-вторых, это незаконно. В-третьих, спрос на данные услуги довольно высокий.*

*Я отдавал себе отчет о всех рисках в черном бизнесе. Знал, к чему это может привести, однако активно тусовался в этой среде. Я знал, что большинство из этих мошенников либо кидалы, либо посредники и лишь небольшой процент реальные продавцы. Возникали мысли, что можно наживаться на этих самых мошенниках. Взламывать псевдо-хакеров, кидать кидал, вымогать у вымогателей. Что может быть лучше? Так скажем, наказывать плохих людей, да еще и получать за это прибыль.*

*Не секрет, что самыми прибыльными в темной стороне интернета были и остаются люди, занимающиеся отмыванием и обналичиванием денег, а также наркодилеры, занимающиеся продажей наркотиков. В целом, изучив «dark web», выбор пал именно на торговцев наркотиков. Изначально использовали они наш любимый корявый skype, старенькую icq, а также jabber и Brosix.*

*Я знал, как взламывать скайпы различными методами, поэтому мы без труда взламывали по 3-5 магазинов в день. Заходя на аккаунт дилера, можно было довольствоваться огромной базой клиентов-торчков. Их количество зависело от репутации магазина. Суть заработка состояла в том, чтобы подменять кошелек магазина на свой, на который оплачивали деньги клиенты. Минимальная стоимость пары грамм синтетических веществ составляла около 1 тысячи рублей. Клиенты были разные и иногда 1 клиент платил до 20 тысяч рублей единовременно. Заработок доходил до 100 тысяч рублей в сутки. Неплохо?*

*Не всегда мы использовали такой грубый метод. Во-первых, клиенты понимали, что их кинули, поэтому клиентская база быстро сокращалась, и*



*магазин быстро умирал. Хмм... Если так подумать, то мы закрываем магазины веществ, рушим бизнес дилеров и получаем к тому же за это деньги. Где в это время было ФСБ и ФСКН? (шутка). Большинство дилеров предлагали за их взломанные аккаунты большой выкуп. Часто мы соглашались и давали дилерам работать дальше, но через некоторое время снова наведывались к ним. Менее чем за полгода все дилеры полностью отказались от скайпа.*

## **Выкуп**

Это один из моих любимых способов, основанных на вымогательстве, но вымогать деньги мы будем у все тех же торговцев веществами. Сразу возникает вопрос, а чем же мы будем их шантажировать?

Широкое использование Киви-кошельков порождало все больше идей и способов взлома. Когда основные методы были прикрыты, то я обратил внимание на один пункт в службе поддержки. Дело в том, что мы могли заблокировать любой киви-кошелек. Причиной служило следующее. Мы пишем текст якобы от себя и просим заблокировать наш киви кошелек, так как потеряли телефон с сим-картой и боимся за свои средства. Служба поддержки любезно блокирует все операции на кошельке, как и сам вход в кошелек. Но есть одно очень важное условие! Если в течение 15 минут не предоставить паспорт и договор на номер кошелька, то кошелек разблокируют. Формально мы можем заблокировать любой кошелек на 15 минут. Как это использовать – я сразу же понял.

Я добавлялся к дилеру в icq и писал, что кошелек заблокирован до тех пор, пока не получу определённую сумму. На этот диалог у меня должно было уйти не более 15 минут, чтобы я смог получить деньги до того, как кошелек разблокируют. Я получаю деньги, проходит пару минут и кошелек снова работает. Если сумма на кошельке действительно большая, то дилер за нее боится, поэтому у него не остается выбора, как заплатить выкуп.

## **Дырка в КИВИ**

Так как основной электронной платежной системой в интернете была Киви, которая остается и сейчас, то большинство кошельков стали активно блокировать. Киви понимала, кто пользуется их системой и ужесточила правила пользования. Во-первых, Киви ввели лимиты на денежные средства. Для этого необходимо было проходить длительную идентификацию. Во-вторых, блокировали кошельки без каких-либо особых причин. А на разблокировку кошелька уходили недели. Для этого были созданы специальные сервисы, предлагающие услуги по разблокировке кошельков.

Они брали определенный процент за эту работу. Заблокированные кошельки попадали и мне, так как я умел пробивать данные и рисовать необходимые документы для разблокировки. Все бы ничего, но разблокировать становилось все труднее и труднее. И тогда я решил проверить одну странную штуку. Я написал в техническую поддержку, что потерял сим-карту и прошу заблокировать временно свой кошелек. Странно, но мне пришел ответ, что тех. поддержка заблокировала номер. Фактически, она заблокировала уже заблокированный кошелек. Я стал ждать. И через 20 минут кошелек разблокировали. Я смог войти под прежним логином и паролем и снять деньги. Я проделал так еще с парой десятков кошельков, после чего киви что-то заподозрила и ответила мне, что не может заблокировать и без того заблокированный номер.

Я считаю, что блокировкой занимался робот, поэтому он не обращал внимания на то, что кошелек изначально был заморожен. Полагаю, что из-за активного обращения по определенной схеме кто-то из сотрудников банка обнаружил эту ошибку и внес корректировки.

**Давайте рассмотрим некоторые интересные разновидности атак на человека.**

✓ *Просим заметить, что все эти случаи реальны и были успешно реализованы.*

## **ПРЯМАЯ АТАКА: ПРОСТО ПОПРОСИ**

Хотите узнать чей-нибудь неопубликованный номер телефона? Социальный инженер может сообщить вам полдюжины способов, но, возможно, самым простым из них будет обычный телефонный звонок, как этот, который мы рассмотрим.

### **Номер, пожалуйста**

Атакующий позвонил по неофициальному номеру телефонной компании, в механизированный центр назначения линий (Mechanized Line Assignment Center). Он сказал женщине, поднявшей трубку:

«Это Пол Энтони, кабельный монтер. Послушайте, здесь загорелась распределительная коробка. Полицейские считают, кто-то пытался поджечь собственный дом, чтобы получить страховку. Я остался здесь заново монтировать целый терминал из двухсот пар. Мне сейчас очень нужна помощь. Какое оборудование должно работать по адресу Саут-Мэйн (South Main), 6723?»

В других подразделениях компании человек, которому позвонили, должен знать, что сведения о неопубликованных номерах предоставляются только уполномоченным лицам. Предполагается, что о центре известно только

служащим компании. И если информация никогда не оглашалась, кто мог отказать в помощи сотруднику компании, выполняющему тяжелую работу? Она сочувствовала ему, у нее самой были нелегкие дни на работе, и она немного нарушила правила, чтобы помочь коллеге с решением проблемы. Она сообщила ему действующий номер и адрес для каждой из кабельных пар.

### **Сообщение от Hacker Place**

В человеческой натуре заложено доверять, особенно когда просьба кажется обоснованной. Социальные инженеры используют это, чтобы эксплуатировать свои жертвы и достичь своих целей.

### **Анализ обмана**

Вы заметите, что в этих историях знание терминологии компании, ее структуры — различных офисов и подразделений, что делает каждое из них и какой информацией владеет — часть ценного багажа приемов успешного социального инженера

## **ВНУШАЯ ДОВЕРИЕ**

Не стоит зазнаваться и верить в то, что все на самом деле полные идиоты, готовые, даже жаждущие, отдать каждый секрет. Социальный инженер знает, что это неправда. Почему атака социальной инженерией так успешна? Это так, не потому что люди глупы или им не хватает здравого смысла... Просто мы, как люди, полностью уязвимы перед обманом, поскольку люди могут изменить доверие, если манипулировать определенным образом. Социальный инженер ожидает подозрение и недоверие, и он всегда подготавливается, чтобы недоверие превратить в доверие. Хороший социальный инженер планирует атаку подобно шахматной игре, предполагая вопросы, которые цель атаки может задать, так что у него могут быть готовы подходящие ответы.

Одна из его основных техник включает создание чувства доверия со стороны его жертв. Как он заставляет Вас верить ему? Поверьте мне, может.

### **Запомните: Доверие: ключ к обману**

Чем естественней социальный инженер общается с жертвой, тем больше он ослабляет подозрение. Когда у людей нет причины для подозрений, социальному инженеру становится легко приобрести доверие жертвы. Как только он получает ваше доверие, разводной мост опускается, и дверь замка распаивается, и он может зайти и взять ту информацию, что он хочет.

### **Одноцентовый сотовый телефон**

Многие люди оглядываются пока не найдут лучшую сделку; социальные инженеры не ищут лучшую сделку, они ищут путь, чтобы сделать сделку выгоднее. Например, иногда компания запускает маркетинговую кампанию, так что вы не можете пропустить ее, пока социальный инженер смотрит на предложение и гадает, как он может улучшить сделку.

Недавно, у национальной сотовой компании была акция: предлагали новый телефон за один цент, если вы подпишете контракт.

Очень много людей обнаружило слишком поздно, что есть много вопросов, которые предусмотрительный покупатель должен спрашивать прежде, чем подписаться на контракт сотовой связи: план услуг аналоговый, цифровой, или комбинированный; количество бесплатных минут в месяц; включена ли в цену плата за роуминг, и так далее. Особенно важно, чтобы понять перед заключением контракта, на сколько месяцев или лет Вы заключаете контракт?

Одного социального инженера в Филадельфии привлек дешевый телефон, предложенный сотовой компанией в контракте, но он ненавидел тарифные планы, которые были в контракте. Не проблема. Вот один путь, по которому он мог управлять ситуацией.

#### **Первый звонок: Тед**

Сначала, социальный инженер звонит в магазин электроники в West Girard.

«Электронный Город. Это Тед.»

"Привет, Тед. Это — Адам. Слушай, Я пару дней назад говорил с продавцом о сотовом телефоне. Я сказал ему что перезвоню, когда решу, какой тарифный план выбрать, и я забыл его имя. Кто тот парень, который работал в этом отделе на днях?

«Тут не один продавец. Это был Вильям?»

«Я не уверен. Может быть, это было Вильям. Как он выглядит?» «Высокий худой парень».

«Я думаю, это был он. Повторите пожалуйста, как его фамилия?»

«Хедли Х—Е—Д—Л—И»

«Да, вроде это был он. Когда он снова будет?»

Я не знаю его расписание на эту неделю, но на вторую смену люди приходят около пяти".

«Хорошо. Я проговорю с ним сегодня вечером. Спасибо, Тед.»

#### **Второй Звонок: Кети**

Следующий звонок — в магазин той же самой компании на North Broad Street.

«Привет, Электронный Город. Кети на проводе, чем могу вам помочь?»

«Кети, Привет. Это — Вильям Хедли, из магазина на West Girard. Как идут сегодня дела?»

«Неважно, а что случилось»

«У меня есть клиент, который пришел по акции “сотовый телефон за один цент”. Знаешь что я имею в виду?»

«Знаю. Я продала пару таких на прошлой неделе».

«У вас еще есть телефоны, которые идут с этой акцией?»

«Получили кучу таких».

«Прекрасно. Я только что продал один клиенту. Парень заплатил кредит; мы подписали с ним контракт. Телефон оказался бракованным, и у нас больше нет ни одного телефона. Я так смущен. Вы можете мне помочь? Я пошлю его в ваш магазин, чтобы приобрести телефон. Вы можете продать ему телефон за один цент? И он обязан перезвонить мне, как только он получит телефон, чтобы я смог ему рассказать про акцию».

«Да, конечно. Пришлите его сюда».

«Хорошо. Его имя Тед. Тед Янеси.»

Когда парень, который называл себя Тедом Янеси, появился в магазине на улице North Broad St. Кети выписала счет и продала сотовый телефон за один цент, так как ее просил коллега. Она попала на трюк мошенника.

Когда пришло время заплатить, покупатель не имел ни цента в кармане, так что он добрался до небольшой тарелки с мелочью у кассового аппарата, взял один, и дал девушке за регистрацию. Он получил телефон, не платя ни одного цента за это.

Теперь он может прийти в другую компанию, которая использует телефоны того же стандарта и заказать себе другой тарифный план без контрактных обязательств.

### **Анализ обмана**

Людям естественно доверять в более высокой степени коллеге, который что-то просит, и знает процедуры компании, жаргон. Социальный инженер в этом рассказе воспользовался преимуществом, узнав детали компании, выдавая себя за служащего компании, и прося помощи в другом филиале. Это случается между филиалами магазинов и между отделами в компании, люди физически разделяются и общаются по телефону, никогда не встречая друг друга.

### **«РАЗРЕШИТЕ ВАМ ПОМОЧЬ»**

Мы все благодарны, когда кто-нибудь со знанием, опытом и желанием помочь приходит и предлагает помочь с проблемами. Социальный инженер понимает это, и знает, как извлечь из этого выгоду.

Он также знает как *создать* вам проблему... а потом сделать вас благодарными, когда он решит проблему... и на вашей поиграв на вашем чувстве благодарности, извлечет из вас информацию или попросит оказать небольшую услугу, которая оставит вашу компанию (или вас лично) в гораздо более плохом состоянии после встречи. И вы можете даже не узнать, что вы потеряли что-то ценное.

Есть несколько типичных способов, которыми социальные инженеры пытаются «помочь».

## **Неполадки в сети**

Дата/Время: Понедельник, 12 февраля, 15:25

Место: Офис кораблестроительной фирмы Starboard.

### **Первый звонок: Том Дилэй**

«Том Дилэй, бухгалтерия».

«Здравствуй, Том, это Эдди Мартин, отдел техпомощи, мы пытаемся найти причины неисправности компьютерной сети. Были ли у кого-либо в вашей группе проблемы с подключением?»

«Нет, я не в курсе».

«А у тебя?»

«Нет, все вроде в порядке».

«Окей, это хорошо. Мы звоним людям, на кого это может повлиять, потому что важно всех проинформировать заранее, если будут внезапные отключения».

«Это звучит нехорошо. Вы думаете, это может случиться?»

«Надеюсь, что нет, но если что случится, позвонишь?»

«Можешь не сомневаться».

«Похоже, отсутствие связи будет для тебя проблемой».

"Бесспорно ".

«Так что пока мы над этим работаем, я дам тебе свой сотовый. Тогда ты сможешь мне все сообщить при первой необходимости».

«Отлично, говори».

«Номер 555 867 5309».

«555 867 5309. Записал. Спасибо. А как тебя зовут?»

"Эдди. И последнее. Мне надо знать, к какому порту подключен твой компьютер. Посмотри, там где-то есть наклейка с надписью «Порт N...»

«Сейчас... Нет, не вижу ничего подобного».

«Ладно, тогда сзади компьютера. Ты узнаешь сетевой провод?»

«Да».

«Тогда посмотри, где он подключен. Там должна быть табличка».

«Подожди секунду. Сейчас. Мне придется туда пролезть, чтобы ее увидеть. Вот. На ней написано Порт 6-47.»

«Отлично, как раз как записано про тебя. Просто проверяю».

### **Второй звонок: Человек из техобслуживания**

Через пару дней поступил звонок в отдел локальной сети.

«Здравствуй, это Боб, я в офисе Тома ДиЛэя из бухгалтерии. Мы пытаемся найти неисправность в кабеле. Надо отключить порт 6-47.»

Человек из техобслуживания сказал, что это будет сделано за несколько минут, и попросил перезвонить, когда потребуется включить порт.

### **Третий звонок: Помощь от врага.**

Примерно через час, человек, представившийся как Эдди Мартин, ходил по магазинам в Circuit City, и вдруг зазвенел телефон. Он посмотрел номер звонящего, узнал, что он из кораблестроительной компании поспешил в спокойное, тихое место, прежде чем ответить.

«Отдел техпомощи, Эдди.»

«О, здравствуй, Эдди. Проблемы со связью. Ты где?»

«Я, э, в кабельной комнате. Кто это?»

«Это Том ДиЛэй. Я рад, что нашел тебя. Может, помнишь, ты мне звонил недавно? Мое соединение не работает, как ты и говорил, и я немножко паникую».

«Да, у нас сейчас отключена куча людей. Но мы все поправим к концу дня. Сойдет?»

«НЕТ! Черт, я серьезно отстану, если я буду отключен столько времени. Никак нельзя побыстрее?»

«Насколько это важно?»

«Пока я могу заняться другими делами. Может, ты все поправишь за полчаса?»

«ПОЛЧАСА? Ну ладно, я брошу то, чем я занимаюсь, и попытаюсь сделать что-нибудь для тебя».

«Я очень благодарен, Эдди!»

### **Четвертый звонок: Попался!**

Через 45 минут...

«Том? Это Эдди. Проверь свое подключение».

Через несколько минут:

«Отлично, оно работает. Великолепно».

«Хорошо, что я смог тебе помочь».

«Да, спасибо большое».

«Слушай, если ты хочешь быть уверен, что твое подключение больше не прервется, надо поставить одну программку».

«Сейчас не лучшее время».

«Я понимаю... Но зато не будет проблем в следующий раз, когда произойдет сбой сети».

«Ну... только если это займет несколько минут».

«Вот что надо сделать...»

Эдди рассказал Тому, как скачать маленькое приложение с одного сайта. После того, как программа скачалась, Эдди сказал запустить ее двойным щелчком мыши. Он попробовал и сказал:

«Не работает. Она ничего не делает».

«Ужас. Наверно, что-то не так с программой. Давай от нее избавимся, и попробуем еще раз в другое время». Он рассказал Тому, как безвозвратно удалить программу.

Затрачено времени: 12 минут.

**Троянский конь** — программа, содержащая хулиганский или вредоносный код, созданная для того, чтобы повредить компьютер или файлы жертвы, или получить данные из компьютера или сети. Некоторые трояны прячутся в ОС компьютера, и смотрят за каждой нажатой клавишей или действием, или принимают команды через сетевое соединение с целью выполнения некоторой функции, и это происходит без ведома жертвы.

И это было еще не все. Он мог вернуться в любое время, и просмотреть электронную почту и личные памятки служащих компании, сделав поиск текста, который сможет показать любые лакомые кусочки информации. Поздно, тем же вечером, когда он обманом заставил свою жертву установить троянского коня, Бобби выкинул свой сотовый в помойку. Конечно, он был осторожен, и очистил память, а потом вытащил батарейку, прежде чем выбросить его — ему меньше всего было надо, чтобы кто-нибудь случайно набрал номер, и телефон зазвонил.

### **Анализ обмана**

Атакующий плетет сети для того, чтобы убедить жертву, что у него есть проблема, которая на самом деле не существует. Или, как в данном случае, проблема, которой пока нет, но атакующий знает, что она *будет*, так как он ее и создаст. Он представил себя человеком, способным найти решение. Организация этого вида атаки особенно привлекательна для атакующего. Из-за того, что все было спланировано заранее, когда «цель» узнает, что у него есть проблема, он звонит и умоляет о помощи. Атакующий просто сидит и ждет, когда зазвонит телефон — эта тактика более известна, как *обратная социальная инженерия*. Атакующий, который может заставить жертву позвонить ему, получает мгновенное доверие: «если я позвоню кому-нибудь, кто, как мне кажется, из технической поддержки, я не буду просить его подтвердить свою личность». В этот момент можно считать, что атакующий уже победил.

**Удаленная командная строка** — Неграфический интерфейс, который принимает текстовые команды для выполнения определенных функций или запуска программ. Атакующий, который эксплуатирует технические уязвимости или может установить Троянского Коня на компьютер жертвы, получает доступ к удаленной командной строке.

**Обратная социальная инженерия** — Социально инженерная атака, в которой атакующий создает ситуацию, где жертва сталкивается с проблемой, и просит атакующего о помощи. Другая форма обратной социальной инженерии переводит стрелки на атакующего. Цель распознает атаку и



использует психологические приемы, чтобы узнать как можно больше информации об атакующем, чтобы бизнес мог направленно охранять свое имущество.

### **Сообщение от Hacker Place**

Если незнакомый человек окажет вам услугу, а потом попросит сделать что-либо, не делайте этого, не обдумав хорошенько то, что он просит.

В афере, подобной этой, социнжинер пытается выбрать такую цель, у которой ограниченные знания в области использования компьютеров. Чем больше он знает, тем больше вероятность того, что он что-то заподозрит, или поймет, что его пытаются использовать. Такой человек, который мало знает о технике и процедурах, «рабочий, бросивший вызов компьютеру», скорее всего, подчинится. Очень вероятно, что он попадет на уловку вроде «Просто скачайте эту программу», потому что даже не подозревает, сколько вреда может принести подобное ПО. Помимо этого, зачастую он не понимает ценности информации, которой он рискует.

Один из наиболее мощных трюков социального инженера включает «перевод стрелок». Это именно то, что вы видели в этой главе. Социальный инженер создает проблему, а потом чудесным образом ее решает, обманом заставляя жертву предоставить доступ к самым охраняемым секретам компании. А ваши сотрудники попадутся на эту уловку? А вы позаботились о создании и применении специальных правил безопасности, которые могли бы предотвратить такое?

### **«НЕ МОГЛИ БЫ ВЫ ПОМОЧЬ?»**

Вы знаете, как социальные инженеры обманывают людей, предлагая им свою помощь. Другой излюбленный подход основан на обратном: социальный инженер делает вид, что нуждается в помощи другого человека. Мы можем сочувствовать людям в затруднительном положении, и подход оказывается эффективным снова и снова, позволяя социальному инженеру достигнуть своей цели.

### **Чужак**

История в главе 3 показала, как атакующий может служащего сообщить свой (табельный) номер. В этой истории применяется другой подход, чтобы добиться того же результата, и показывает, как атакующий может им воспользоваться.

### **Наравне с Джонсами**

В Силиконовой долине есть некая мировая компания, название которой упоминаться не будет. Отделы сбыта и другие подразделения,

расположенные по всему миру, соединены со штаб-квартирой компании посредством глобальной сети (WAN). Взломщик, проворный малый по имени Брайан Аттерби (Brian Atterby), знал, что почти всегда легче проникнуть в сеть в одном из отдаленных мест, где уровень безопасности должен быть ниже, чем в головном офисе.

Взломщик позвонил в офис в Чикаго и попросил соединить с мистером Джонсом. Секретарь в приемной спросила, знает ли он имя мистера Джонса; он ответил: «Оно где-то здесь, я ищу его. Сколько у вас работает Джонсов?». Она сказала: «Три. В каком он подразделении?» Он сказал: «Если вы зачитаете мне имена, может, я вспомню его».

— Барри, Джозеф и Гордон.

— Джо. Я вполне уверен, что это он. И... в каком он подразделении?

— Развития бизнеса

— Отлично. Соедините меня с ним, пожалуйста.

Она соединила его. Когда Джонс взял трубку, атакующий сказал: «Мистер Джонс? Это Тони из отдела (начисления) заработной платы. Мы как раз выполняем ваш запрос о переводе ваших денег на кредитный счет».

— ЧТО?! Вас обманули. Я не делал таких запросов. У меня даже нет счета.

— Проклятие, я уже выполнил запрос.

Джонс был в смятении от мысли, что его деньги могли отправиться на чей-нибудь счет, он начал думать, что парню на том конце провода не следовало торопиться. Прежде чем он успел ответить, атакующий сказал: «Я понимаю, что произошло. Изменения вносятся по номеру служащего. Какой у вас номер?»

Джонс сообщил свой номер. Звонивший сказал: «Действительно, вы не делали запрос».

«Они становятся все более бестолковыми с каждым годом», — подумал Джонс.

«Я внесу исправление прямо сейчас. Не беспокойтесь, вы получите вашу зарплату без проблем», — заверил парень.

### **Командировка**

Почти сразу после этого позвонили системному администратору в отдел сбыта в Остине, Техас.

«Это Джозеф Джонс, — представился звонивший. — Я из отдела развития бизнеса. Я буду в отеле Дрискилл (Driskill Hotel) через неделю. Мне нужна временная учетная запись, чтобы я мог получать электронную почту, не делая междугородных звонков».

«Повторите имя и сообщите мне свой номер», — сказал системный администратор. Лже-Джонс дал ему номер и продолжил: «У вас есть высокоскоростные номера?».

«Подожди, приятель. Я должен проверить тебя по базе данных». Через некоторое время он сказал: «О.К., Джо. Скажи мне номер дома».

Атакующий тщательно подготовился и держал ответ наготове.

### **Сообщение от Hacker Place**

Не надейтесь, что сетевая защита и брандмауэры защитят вашу информацию. Следите за самым уязвимым местом. В большинстве случаев вы обнаружите, что уязвимость заключается в ваших людях.

«О.К., — сказал системный администратор, — ты убедил меня».

Это было просто. Системный администратор проверил имя «Джозеф Джонс», подразделение, номер, и «Джо» сообщил ему правильный ответ на тестовый вопрос. "Имя пользователя будет таким же, как и корпоративное, «jbjones», — сказал системный администратор, — и начальный пароль «changeme» («смени меня»).

### **Анализ обмана**

С помощью пары звонков и 15 минут атакующий получил доступ к глобальной сети компании. В этой компании, как и во многих организациях, было то, что я называю «*слабой безопасностью*» (candy security), термином впервые использованным двумя исследователями из Bell Labs, Стивом Белловином (Steve Bellovin) и Стивенсом Чесвиком (Steven Cheswick). Они описывали такую безопасность как «крепкая оболочка со слабым центром», похожую на конфеты M&M. Белловин и Чесвик доказывали, что внешней оболочки, брандмауэра, недостаточно для защиты, потому что взломщик способен обойти ее, а внутренние компьютерные системы защищены слабо. В большинстве случаев они защищаются недостаточно надежно.

Данная история подходит под определение. Имея номер для удаленного доступа и учетную запись, атакующему даже не надо было беспокоиться о проникновении через брандмауэр Интернет, и, будучи внутри, он легко мог скомпрометировать большинство систем во внутренней сети.

По моим данным, эта хитрость сработала с одним из крупнейших производителей компьютерных программ. Вы подумаете, что системных администраторов таких компаний, вероятно, учат обнаруживать уловки такого типа. Мой опыт подсказывает, что никто полностью не защищен от способного и убедительного социального инженера.

**«Слабая безопасность» (candy security)** — термин, введенный Белловином и Чесвиком из Bell Labs для описания сценария безопасности, где внешняя граница, такая как брандмауэр, прочна, но инфраструктура, расположенная за ним, слаба.

**Speakeasy security** — «прозрачная» безопасность, которая основана на знании, где находится нужная информация, и использовании слова или имени для доступа к информации или компьютерной системе.

### **«Прозрачная» безопасность (Speakeasy security)**

В дни существования — ночных клубов (speakeasies), где разливался джин — потенциальный клиент получал доступ, найдя дверь и постучав в нее. Через несколько минут, открывалось маленькое окошко и показывалось

устрашающее бандитское лицо. Если посетитель был «своим», он называл имя завсегдатая (часто было достаточно сказать: «меня отправил Джо»), после чего вышибала открывал дверь и разрешал войти. Хитрость была в том, что нужно было знать, где находится заведение, так как дверь ничем не выделялась, и хозяева не размещали вывеску, указывающую на свое присутствие.

### **Я видел это в фильмах**

Вот пример из известного фильма, который многие люди помнят. В *"Трех днях Кондора"* главный герой Тернер (роль играет Роберт Рэдфорд) работает с небольшой исследовательской фирмой по контракту с ЦРУ. Однажды он возвращается с обеда и обнаруживает, что всех его сотрудников застрелили. Ему нужно было выяснить, кто это сделал и почему, зная, что в это время те плохие парни разыскивают его.

Позже он сумел узнать телефонный номер одного из парней. Но кто он такой и как найти его? Ему повезло: сценарист, Дэвид Рэйфил, к счастью, снабдил его опытом, который включает подготовку в войсках связи, дающую ему представление о работе телефонных компаний. Располагая номером парня, Тернер точно знает, что нужно делать дальше. В фильме сцена выглядит таким образом:

Тернер повторно соединяется и набирает другой номер  
звонок! звонок! Затем:

**Женский голос (фрагмент).** Служба имен и адресов (CNA — Customer Name and Address bureau). Миссис Колеман.

**Тернер.** Миссис Колеман, это Гарольд Томас, абонентская служба. Имя и адрес абонента, пожалуйста, для 202-555-7389.

**Женский голос (фрагмент).** Одну минуту.  
(почти сразу)

Леонард Этвуд, Маккензи Лэйн, 765, Мэриленд. (Leonard Atwood, 765 MacKensie Lane, Chevy Chase, Maryland).

Можете вы осознать случившееся, не обращая внимания на то, что сценарист ошибочно использует междугородный код Вашингтона, округ Колумбия, для адреса в Мэриленде?

Тернер, благодаря опыту линейного монтера, знает, по какому номеру надо звонить в офис компании, которая называется «Служба имен и адресов».

Служба имен и адресов абонентов предназначена для удобства монтажников и другого персонала компании. Монтажник может позвонить в службу и назвать номер. Служащий сообщит имя и адрес человека, которому принадлежит телефон.

### **Обман телефонной компании**

В реальной жизни номер службы имен и адресов — тщательно охраняемая тайна. Хотя телефонные компании в наши дни не так легко предоставляют информацию, в то же время они используют разновидность «прозрачной»

безопасности, которую специалисты по безопасности называют «*security through obscurity*» (безопасность, основанная на незнании). Предполагается, что любой, кто позвонил в службу имен и адресов и владеет соответствующей терминологией (например, «имя и адрес для 555-1234, пожалуйста»), является человеком, имеющим право на получение информации.

### **Lingo**

**SECURITY THROUGH OBSCURITY** — неэффективный метод компьютерной безопасности, основанный на содержании в тайне деталей работы системы (протоколы, алгоритмы, внутренние системы). Такая безопасность основана на обманчивом предположении, согласно которому никто за пределами группы посвященных людей не способен обойти систему.

### **Сообщение от Hacker Place**

Безопасность, основанная на незнании, не приносит никакой пользы при отражении атак социальной инженерии. В каждой компьютерной системе в мире есть как минимум один человек, который ее использует. Таким образом, если социальный инженер способен манипулировать людьми, использующими системы, незаметность системы не подходит.

Не нужно было подтверждать свою личность, сообщать свой номер, ежедневно изменяемый пароль. Если вы знали номер и говорили достоверно, то должны получить право на информацию.

Это было не очень основательным предположением со стороны телефонной компании. Единственная мера безопасности, которую они предприняли, — периодическая смена телефонного номера, по крайней мере, раз в год. Несмотря на это, действующий номер в определенный момент времени был широко известен среди фрикеров, использующих этот удобный источник информации в своих кругах. Хитрость со службой имен и адресов абонентов была одной из первых вещей, которые я изучил во время увлечения фрикингом в юношеском возрасте.

В мире бизнеса и правительства все еще преобладает «прозрачная» безопасность. Вероятно, здесь необходимо обладать знаниями о подразделениях, людях, и терминологии. компании. Иногда все, что требуется знать, — это внутренний телефон.

## **ФАЛЬШИВЫЕ САЙТЫ И ОПАСНЫЕ ПРИЛОЖЕНИЯ**

Говорят, что вы никогда не получите ничего просто так.

По-прежнему, предложение чего-либо бесплатного является хорошей уловкой для получения больших доходов в законном ("Но подождите, это еще не всё! Позвоните прямо сейчас и вы получите дополнительно набор ножей!") и не совсем законном («Купите один акр заболоченных земель во Флориде и второй вы получите бесплатно!») бизнесе.

И большинство из нас так горит желанием получить это что-то, что многих может сбить с толку, заставить не анализировать это предложение или данное обещание.

Мы знаем привычное предупреждение, «предостережение покупателя», но пришло время обратить внимание на другое предупреждение:

Остерегайтесь приложений во входящей почте и свободного программного обеспечения. Сообразительный взломщик использует любое доступное средство, чтобы вломиться в корпоративную сеть, включая обращение к нашему естественному желанию получить бесплатный подарок. Вот вам несколько примеров.

### **«Не желаете ли вы бесплатно ...?»**

Также как и вирусы стали бедствием для человечества и врачей с начала времен, так и подходяще названный компьютерный вирус представляет собой ту же угрозу для пользователей современных технологий.

Компьютерные вирусы, которые привлекают к себе внимание и прекращаются, как только становятся в центре внимания, не случайно наносят большой урон. Они являются продуктом компьютерных вандалов. Люди, очень интересующиеся компьютерами, становятся злобными компьютерными вандалами, прилагающими все усилия, чтобы показать, насколько они умны. Иногда их действия похожи на обряд инициации, предназначенный для того, чтобы произвести впечатление на старших и более опытных хакеров. Главной мотивацией этих людей в написании червей или вирусов является преднамеренное нанесение ущерба. Если их деятельность уничтожает файлы, разрушает полностью жесткие диски, и самостоятельно рассылается тысячам ничего не подозревающих людей, то вандалы раздуваются от гордости за свое достижение. Если вирус вызывает достаточный хаос, чтобы о нем написали в газетах и предупреждения были даже в сети — это еще лучше.

Много написано о вандалах и их вирусах; книги, программное обеспечение и целые компании были созданы, чтобы обеспечить защиту, но мы не будем пытаться выдвигать аргументы против их атак. В данный момент, разрушительные действия вандалов интересуют нас меньше, чем запланированные действия его дальнего родственника — социального инженера.

### **Это пришло в письмо**

Скорей всего, вы каждый день получаете неожиданные письма, которые содержат в себе рекламные объявления или предложения чего-либо, в чем вы не только не нуждаетесь, но и не хотите. Думаю, вы знакомы с этим. Они

обещают советы по размещению капитала, скидки на компьютеры, телевидение, камеры, витамины или путешествия, предлагают кредитные карты, которые вам не нужны, устройство, которое позволит вам бесплатно смотреть платные каналы, пути улучшения вашего здоровья или сексуальной жизни и так далее, и так далее. Но всегда в вашем электронном ящике найдется сообщение, которое заинтересует вас. Может быть, это бесплатная игра или предложение посмотреть фотографии вашего кумира, бесплатный список программ или недорогая условно-бесплатная программа, которая защитит ваш компьютер от вирусов. Что бы ни предлагалось, вам придется скачать файл с товарами, которые это сообщение убеждает вас попробовать. Или, может быть, вы получаете сообщение с темой «Дон, я соскучилась» или «Анна, почему ты мне не пишешь» или «Привет Тим, это та сексуальная фотография, которую я обещал». Это не может быть ненужным рекламным письмом, думаете вы, потому что оно содержит ваше имя и кажется таким личным. И вы запускаете приложение, чтобы увидеть фотографию или прочитать сообщение.

Все эти действия — загрузка программы, о которой вы узнали в рекламном письме, щелканье по ссылке, которая отправит вас на сайт, о котором вы раньше не слышали, запуск приложения от кого-то, кто вам незнаком — это своеобразное начало проблем. Конечно, чаще всего, то, что вы получаете — это то, что вы ожидали или в худшем случае, что-либо отменяющее или обидное, но безопасное. Но иногда то, что вы получаете — это дело рук вандала.

Умышленная отправка вредоносного кода на ваш компьютер — это всего лишь малая часть атаки. Атакующий должен, прежде всего, убедить вас скачать приложение, чтобы атака удалась.

### **Заметка**

Одним из типов программ, хорошо известных в компьютерном подполье, является утилита удаленного администрирования или троян, который дает взломщику полный контроль над вашим компьютером, как будто он сам сидит за вашей клавиатурой.

Наиболее опасные формы вредоносного кода-это черви типа LoveLetter, SirCam и Anna Kournikova, все они основаны на технике социального инжиниринга и обмане, нашего желания получить что-то просто так. Червь приходит как приложение к письму, предлагающему что-то соблазнительное, например конфиденциальную информацию, бесплатную порнографию или (очень умная уловка) сообщение, в котором говорится, что файл является распиской за какой-то дорогой товар, который вы, предположительно, заказали. Эта последняя хитрость ведет к тому, что вы открываете файл из страха, что с вашей кредитки может быть снята сумма за товар, который вы не заказывали.

Это поразительно, как много людей попадает на эти уловки, даже будучи предупрежденными об опасности запуска приложений; осведомленность об опасности со временем исчезает, оставляя нас уязвимыми.

### **Определение вредоносных программ.**

Другой вид *malware* — вредоносное программное обеспечение, которое добавляет на ваш компьютер программу, работающую без вашего ведома или согласия, или выполняющую задание без предупреждения. Malware могут выглядеть достаточно безобидно, быть, например, документом Word или PowerPoint презентацией или другим документом, имеющим много функций, но они инсталлируют неразрешенную программу. Например, malware может быть одной из версий Трояна, о котором мы говорили в Главе 6. Будучи однажды установленной на ваш компьютер, она может отправлять всю набранную вами информацию, включая пароли и номера кредиток, взломщику.

Существует два других типа вредоносных программ, которые могут шокировать вас. Программа первого типа может отправлять взломщику каждое сказанное вами в микрофон слово, *даже если вы думаете, что он выключен*. Хуже, если у вас есть веб-камера, тогда взломщик может захватить все, что попадает в обзор напротив вашего терминала, даже если вы думаете, что камера не работает.

**Malware** — на сленге: вредоносные программы, такие как вирус, червь, троян, которые наносят повреждения

### **Сообщение от Hacker Place**

Бойтесь греков, дары приносящих, иначе вашу компанию может постигнуть участь города Трои. Если у вас есть сомнения, то лучший способ избежать заражения — использовать защиту.

Хакер со злобным чувством юмора может внедрить вам маленькую программку, которая доставит много хлопот вашему компьютеру. Например, она может заставить открываться ваш CD-rom или свернуть файл, с которым вы только что работали. Также это может быть аудио запись крика на полной громкости посреди ночи. Ничто из вышеперечисленного не покажется вам смешным, если вы пытаетесь поспать или выполнить свою работу... но, тем не менее, они не причиняют урона.

### **Сообщение от друга**

Сценарий может развиваться еще хуже, несмотря на ваши предосторожности. Представьте себе: Вы решили не давать взломщику



больше ни единого шанса. Вы больше не собираетесь скачивать какие-либо файлы, за исключением файлов с безопасных сайтов, которым вы доверяете, таких как SecurityFocus.com или Amazon.com. Вы больше не кликаете по ссылкам в электронных письмах от неизвестных адресатов. Вы больше не запускаете приложений в письмах, которые вы не ждали. И вы проверяете страницу вашего браузера, чтобы убедиться, что сайты, которые вы посещаете с целью коммерческих транзакций или обмена конфиденциальной информацией, обладают должным уровнем защиты. И однажды вы получаете письмо от друга или делового партнера, которое содержит приложение. Ведь не может что-то опасное прийти от человека, которого вы знаете, правда? Особенно, если вы знаете, кого винить, если информация на вашем компьютере была повреждена.

Вы запускаете файл и... БУМ! Ваш компьютер только что был заражен червем или трояном. Но зачем такой поступок будет совершать человек, которого вы знаете? Потому что не все в этом мире так, как нам кажется. Вы читали об этом: червь проник в чей-то компьютер и разослался всем, кто был записан в адресной книге. Каждый из тех людей получил письмо от кого-то, кого он знал и кому верил, и каждое из этих писем содержало в себе червя, который самостоятельно распространялся, как рябь по глади озера от брошенного камня.

Причина, почему этот метод является таким эффективным, заключается в том, что он следует теории о попадании в двух птиц одним камнем: умение самостоятельно распространяться и вероятность, что оно приходит от известного вам человека.

### **Сообщение от Hacker Place**

Человечество изобрело много замечательных вещей, которые перевернули мир и нашу жизнь. Но на каждое нормальное пользование технологиями, будь то компьютер, телефон или Интернет, кто-то всегда найдет способ злоупотреблять ими в его или ее интересах.

Печально, что, несмотря на высокий уровень развития современных технологий, вы можете получить письмо от кого-то, близкого вам, и все еще думать, а безопасно ли его открыть.

### **Вариации по теме**

В эту эру Интернета, существует вид мошенничества, который перенаправляет вас совсем не на тот веб-сайт, который вы ожидали. Это случается регулярно и имеет разнообразные формы проявлений. Этот пример является типичным.

## **С Новым Годом...**

Отставной страховой агент по имени Эдгар получил письмо от PayPal, компании, которая предоставляла быстрый и удобный путь совершения онлайн покупок. Этот вид сервиса очень удобен, когда человек из одной части страны (или мира) покупает что-либо у человека, с которым он не знаком. PayPal снимает деньги с кредитки покупателя и переводит деньги прямо на счет продавца. Будучи коллекционером антикварных стеклянных кружек, Эдгар совершил множество сделок через он-лайн торги eBay. Он часто пользовался PayPal, иногда несколько раз в неделю. В общем, Эдгар был заинтересован в получении письма на выходных 2001 года, которое, казалось, было отправлено от кого-то PayPal, предлагающего ему награду за обновления своего PayPal счета. В письме было написано:

Сезонные поздравления нашим дорогим клиентам PayPal;  
В честь прихода Нового Года PayPal желает добавить 5\$ на ваш счет!  
Все, что вам требуется, чтобы получить в подарок 5\$-обновить вашу информацию на защищенном сайте PayPal к 1 Января, 2002. Год приносит много изменений и, обновив вашу информацию, вы позволите нам продолжать предоставлять вам и другим дорогим клиентам сервис отличный сервис и, между тем, неуклонно придерживайтесь нашей инструкции!  
Чтобы обновить вашу информацию прямо сейчас и получить 5\$ на ваш PayPal аккаунт, щелкните по этой ссылке: <http://www.paypal-secure.com/cgi-bin>  
Благодарим вас за использование PayPal.com и помощь в дальнейшем развитии нашей компании!  
От всего сердца желаем вам счастливого Нового Года!  
команда PayPal

## **Заметка о коммерческих веб сайтах**

Возможно, вы знаете людей, вынужденных покупать товары он-лайн, даже у таких брендовых компаний, как Amazon и eBay или веб сайтах Old Navy, Target или Nike. По сути дела, они имеют право быть подозрительными. Если ваш браузер использует сегодняшний стандарт 128 битного шифрования, то информация, которую вы посылаете какому-нибудь защищенному сайту, выходит из вашего компьютера зашифрованной. Эта информация может быть расшифрована с большим трудом, но, в принципе ее невозможно взломать разумные сроки, кроме, разве что привлечения Национального Агентства Безопасности (и оно, насколько нам известно, в 98 году, совсем не показало свой заинтересованности в краже номеров кредиток американцев или попытке выяснить, кто заказывает порно-фильмы или странное нижнее белье).

Эти зашифрованные файлы могут быть вскрыты кем-то лишь при достаточном наличии времени и ресурсов. Но реально, какой дурак пойдет

на все это, чтобы украсть один номер кредитки, когда множество онлайн компаний совершают ошибку, храня всю финансовую информацию их клиентов незашифрованной в базах данных? Хуже всего то, что достаточное количество таких компаний, которые используют обычную базу данных SQL, плохо разбираются в проблеме. Они никогда не меняют стоящий по умолчанию пароль системного администратора в программе. Когда они доставали программное обеспечение из коробки, пароль был «null», и он по-прежнему «null» сегодня. Так что содержимое базы данных доступно любому в Интернете, кто решит попробовать подсоединиться к серверу базы данных. Эти сайты все время атакуются, и информация воруются, так как нет никого более опытного.

С другой стороны, те же самые люди, которые не делают покупки через Интернет, потому что боятся кражи информации о своей кредитке, не имеют проблем при использовании той же кредитки в обычном магазине, уплате за ланч, ужин или выпивку. Чеки о снятии денег с кредитки крадутся из этих мест постоянно или вылавливаются из мусорных корзин на заднем дворе. И любой недобросовестный клерк или официант может записать ваше имя и информацию о карте или использовать приспособление, легко доступное в Интернете, или устройство, которое считывает информацию с любой кредитки, как только ей проведут через него, для дальнейшего восстановления.

Существуют несколько опасностей в совершении покупок он-лайн, но, возможно, это так же безопасно, как и в обычных магазинах. И компании, обслуживающие кредитки, предоставляют вам ту же защиту, когда вы пользуетесь своей картой он-лайн, если было совершено незаконное снятие денег с вашего счета, вы несете ответственность только за первые 50\$. Так что, по-моему, страх покупок в Интернете — это еще одно необоснованное беспокойство.

Эдгар не заметил некоторых особенных знаков, которые были неправильны в этом письме (например, точка с запятой после поздравительной строки и опечатку « дорогим клиентам сервис отличный сервис»). Он щелкнул по ссылке, заполнил информационный запрос — имя, адрес, номер телефона, информацию о кредитке — и сел ждать, когда же 5\$ поступят на его счет. Но вместо того, начал появляться список расходов на товары, которые он никогда не заказывал.

### **Анализ обмана**

Эдгар попался на довольно банальный в Интернете трюк. Это трюк, который можно использовать довольно разнообразно. Один из видов (описан в Главе 9) включает в себя макет формы авторизации, созданный взломщиком, и идентичный настоящему. Разница заключается в том, что фальшивая форма не дает доступа к системе, до которой пользователь пытается добраться, а кроме этого, отправляет его логин и пароль хакеру.

Эдгар попался на трюк, в котором обманщики зарегистрировали веб сайт с именем «paypal-secure.com»-который звучит так, будто бы это защищенная страница законного PayPal сайта, но это не так. Когда он ввел информацию на том сайте, взломщики получили то, что хотели.

### **Сообщение от Hacker Place**

Пока отсутствует полная защищенность, всякий раз, когда вы посещаете сайт, который требует информацию, которую вы считаете личной, убедитесь, что соединение подлинно и зашифровано. И еще более важно не щелкать автоматически «Да» в любом диалоговом окне, которое может отображать информацию о безопасности, такую как неверный, истекший или аннулированный цифровой сертификат.

## **СОЧЕТАЯ ТЕХНОЛОГИЮ И СОЦИАЛЬНУЮ ИНЖЕНЕРИЮ**

Социальный инженер живет своей возможностью манипулировать людьми, заставляя делать то, что поможет ему достичь своей цели, но успех обычно требует большого количества знаний и навыков в использовании компьютеров и телефонных систем.

### **Взлом решетки**

Какие системы вы можете вспомнить, защищенные от взлома — физического, телекоммуникационного или электронного? Форт Нокс ? Конечно. Белый Дом? Абсолютно точно. NORAD (North American Air Defence), Северно-американская воздушно-защитная база, расположенная глубоко под горой? Определенно.

А как насчет тюрем и мест заключений? Они должны быть не менее безопасны, чем другие места в стране, верно? Люди редко убегают, и даже если это им удастся, их обычно вскоре ловят. Вы можете думать, что государственная организация будет неуязвима для атак социальных инженеров. Но вы будете не правы — нигде нет такой вещи, как «защита от дурака».

Несколько лет назад, пара профессиональных мошенников столкнулись с проблемой. Так получилось, что они унесли большую сумку наличных у местного судьи. У этой пары уже не первый год были проблемы с законом, но сейчас федеральные власти особо заинтересовались. Они поймали одного из мошенников, Чарльза Гондорффа, и посадили его в исправительную колонию рядом с Сан-Диего. Федеральный судья приказал удерживать его как угрозу обществу и потенциального беглеца.

Его друг Джонни Хукер знал, что для Чарли потребуется хороший адвокат. Но откуда взять деньги? Как и у многих других мошенников, все его деньги уходили на хорошую одежду, модные машины и женщин так же быстро, как и приходили. Джонни с трудом хватало денег на проживание.

Деньги на адвоката должны были прийти после очередного дела. Джонни не собирался делать все самостоятельно. Чарли Гондорфф всегда планировал все их аферы. Но Джонни даже не смел зайти в исправительную колонию, чтобы спросить у Чарли, что делать, учитывая то, что федералы знали, что в преступлениях участвовали двое, и жаждали заполучить второго. Только члены семьи могли посещать заключенных, что означало, что ему пришлось бы воспользоваться фальшивым удостоверением, утверждая, что он — член семьи. Пытаться использовать фальшивое удостоверение личности в федеральной тюрьме — не самая разумная идея.

Нет, ему надо было как-то связаться с Гондорффом.

Это будет нелегко. Ни одному заключенному из федеральной, штатной или местной организации не позволено отвечать на звонки. Над каждым телефоном в федеральной колонии висят таблички, на которой может быть написано, к примеру, «Предупреждаем вас, что все Ваши разговоры с этого телефона будут подвергнуты прослушиванию, и использование этого телефона означает согласие с прослушиванием». Правительственные работники будут слушать ваши звонки, когда совершение преступления — это способ продления государственно-оплачиваемого отпуска.

Джонни знал, что некоторые звонки не прослушиваются: звонки между заключенным и его адвокатом — отношения, защищенные Конституцией, к примеру. Вообще то, учреждение, где задерживался Гондорфф, было соединено напрямую с Офисом общественных Защитников (ООЗ). Поднимая один из телефонов, устанавливается прямое соединение с ООЗ. Телефонная компания называет это *прямой линией*. Ничего не подозревающая администрация полагает, что эта служба безопасна и неуязвима для вторжения, потому что исходящие звонки поступают только в ООЗ, а входящие звонки блокируются. Даже если кто-либо как-либо узнает номер, он запрограммирован в телефонной компании на *deny terminate* (*запрет прекращения*), неуклюжий термин телефонных компаний для услуги, где запрещены входящие звонки.

Поскольку любой достойный мошенник отлично разбирается в искусстве обмана, Джонни понял, что можно решить эту проблему. Изнутри, Гондорфф уже пытался поднимать трубку и говорить: «это Том, из ремонтного центра компании. Мы проверяем эту линию, и мне надо, чтобы вы набрали 9, а потом 00». Девятка открыла бы доступ на внешние линии, а ноль-ноль бы соединили с оператором по дальним звонкам. Но это не сработало — человек, ответивший на вызов, уже знал этот трюк.

Джонни был более успешен. Он уже узнал, что в тюрьме есть десять жилых отделений, каждое с прямой линией к Офису Общественных Защитников. Джонни встретил несколько препятствий, но как социальный инженер, он знал, как преодолеть эти раздражающие камни преткновения. В каком именно отделении был Гондорфф? Какой был номер у службы прямого соединения с этим отделением? И как ему передать его первое сообщение Гондорффу, чтобы оно не было перехвачено тюремными властями? То, что может показаться невозможным для среднестатистического человека, как получение секретных номеров, расположенных в государственных заведениях, — не более чем несколько звонков для афериста. После пары бессонных ночей мозговой атаки, Джонни проснулся однажды утром с полным планом в голове, состоящим из пяти пунктов. Во-первых, надо узнать номера десяти отделений, соединенных с ООЗ. Все 10 надо изменить на прием входящих вызовов. Потом надо узнать, в каком отделении Гондорфф задерживается. После этого надо выяснить, какой номер соединен с этим отделением. И, наконец, договориться с Гондорффом о звонке так, чтобы правительство ничего не заподозрило.

*Лакомый кусочек* , подумал он.

## LINGO

**Прямое соединение** — Термин телефонных компаний для телефонной линии, которая соединяется с определенным номером когда поднята трубка.

**Deny Terminate** — Сервис телефонной компании, где оборудование настроено так, что входящие звонки не могут быть приняты с определенного номера.

**Звоню в Ma Bell** (американская телеф. компания — прим. пер.)

Джонни начал со звонков в офис телефонной компании под видом сотрудника гособслуживания, организации, ответственной за приобретение товаров и услуг для правительства. Он сказал, что работает над заказом по покупке дополнительных услуг, и хотел получить счета по всем используемым прямым линиям связи, включая рабочие номера и телефонную стоимость в тюрьме Сан-Диего. Женщина была рада помочь. Чтобы убедиться, он попробовал набрать один из номеров, и ответил типичный голос с записи: «Эта линия отключена или не обслуживается». На самом деле ничего подобного не имелось в виду, это означало, что линия запрограммирована блокировать входящие звонки, как он и ожидал. Он знал из его обширных знаний об операциях и процедурах телефонных компаний, что ему придется дозвониться до департамента Recent Change Memory Authorisation Center или RCMAC (Я всегда буду задавать себе вопрос — кто придумывает эти названия! Действительно необычно — это переводится как "Уполномоченный Центр Частой Смены Памяти " — прим. пер.). Он начал со звонка в коммерческий офис фирмы, сказал, что он из

отдела ремонта и хотел узнать номер центра RCMAC, который обслуживал зону с названным им с кодом и префиксом, и он оказался тем же офисом, обслуживающим все линии тюрьмы. Эта была самая обычная услуга, предоставляемая техникам на работе, нуждающимся в помощи, и служащий незамедлительно дал номер.

Он позвонил в RCMAC, назвал «телефонное» имя и опять сказал, что он из отдела ремонта. Когда женщина ответила, Джонни спросил: «Установлен ли на номере deny terminate?»

«Да» — сказала она.

"Тогда это объясняет, почему клиент не может получать звонки..." — сказал Джонни. «Слушай, окажи мне, пожалуйста, услугу. Надо изменить свойство линии или убрать запрет входящих, ладно?» Возникла пауза, пока она проверяла другую компьютерную систему, есть ли приказ, разрешающий изменение. «Этот номер должен запрещать входящие звонки. Нет приказа об изменении».

«Тогда это ошибка... Мы должны были передать приказ вчера, но представитель счета заболела, и забыла попросить кого-либо отнести приказ за нее. Так что теперь клиентка бурно протестует по этому поводу».

После секундной паузы женщина обдумала просьбу, ведь просьба необычна и противоречит стандартным операциям, и сказала «Ладно». Он слышал, как она печатает, внося изменения. И через несколько секунд, все было сделано. Лед тронулся, между ними образовалось нечто, похожее на сговор. Поняв отношение женщины и ее желание помочь, Джонни, не колеблясь, решил попробовать все сразу. Он сказал: «У тебя есть еще пару минут, чтобы помочь мне?»

«Да, — она ответила, — Что вам надо?»

«У меня есть еще пару линий, принадлежащих той же клиентке, и на всех та же проблема. Я прочту вам номера, чтобы вы проверили, поставлен ли на них запрет входящих — хорошо?» Она согласилась.

Через несколько минут, все линии были «починены» на прием входящих звонков.

### **Поиск Гондорффа**

Теперь ему надо было узнать, в каком отделении находится Гондорфф. Это информация, которую люди, содержащиеся в местах заключения и тюрьмы, точно не захотят предоставить посторонним. Снова Джонни должен был положиться на свои навыки в социальной инженерии.

Он решил позвонить в тюрьму другого города — Майами, но любой другой бы подошел, и сказал, что он звонит из Нью-йоркской тюрьмы. Он попросил кого-нибудь, кто работает с компьютером центрального бюро, содержащего информацию обо всех заключенных, содержащихся в тюрьмах по всей стране.

Когда человек подошел к телефону, Джонни заговорил на своем Бруклиновском акценте. «Привет, — он сказал, — Это Томас из FDC (Federal detention center), Нью-Йорк. Наше подключение с центральным бюро не работает, не могли бы вы посмотреть расположение преступника для меня, мне кажется, он может быть в вашем учреждении», — и он сказал имя Гондорффа и регистрационный номер.

«Нет, он не здесь,» — сказал парень через несколько секунд. «Он в исправительном центре в Сан-Диего».

Джонни притворился удивленным. «Сан-Диего! Его должны были переправить в Майами на судебном самолете на прошлой неделе! Мы говорил об одном человеке — какая у него дата рождения?»

«12/3/60» сказал мужчина, прочитав с экрана.

«Да, это тот парень. В каком отделении он находится?»

«Он в Северном-10», сказал мужчина, беззаботно ответив на вопрос, не смотря на то, что не было уважительной причины, зачем эта информация понадобилась работнику в Нью-Йорке.

Сейчас у Джонни были телефоны, включенные на прием входящих, и знал, в каком отделении находится Гондорфф. Теперь надо узнать, какой номер подключен к отделению Северное-10.

Это — сложная часть. Джонни позвонил на один из номеров. Он знал, что звонок телефона будет выключен; никто не узнает, что он звонит. Так что он сидел и читал туристический справочник *Величайшие Города Европы Фодора (Fodor's Europe's Great Cities)*, слушая постоянные гудки в телефоне, пока наконец-то кто-то не поднял трубку. Заключение на другом конце линии, конечно, будет пытаться добраться до своего адвоката, назначенного судом. Джонни подготовил ответ. "Офис Общественных Защитников, " — он объявил.

Когда мужчина попросил своего адвоката, Джонни сказал: «Я посмотрю, свободен ли он. Вы из какого отделения?» Он записал ответ мужчины, щелкнул по hold, вернулся через полминуты и сказал: «Он сейчас в суде, вам придется перезвонить позднее».

Он потратил большую часть утра, но могло быть и хуже; его четвертая попытка оказалась Северной-10. Теперь Джонни знал номер, соединенный с ООЗ в отделении Гондорффа.

### **Синхронизируй свои часы**

Теперь надо передать сообщение Гондорффу, когда ему надо поднять трубку, подключенную к Офису Общественных Защитников. Это было проще, чем может показаться.

Джонни позвонил в тюрьму, используя «официально — звучащий» голос, представился как сотрудник, и попросил, чтобы его соединили с Северным-10. Звонок соединили. Когда надзиратель поднял там трубку, Джонни обманул его, используя внутреннюю аббревиатуру для Приема и Выпуска



(Recieving and Discharge), отдела, который работает с новыми и отбывающими заключенными: «Это Томас из П&В,» сказал он. «Я должен поговорить с заключенным Гондорффом. У нас есть некоторые его вещи, и он должен сообщить нам адрес, куда нам их лучше отправить. Не могли бы вы его позвать к телефону?»

Джонни слышал, как охранник кричит через комнату. Через несколько нетерпеливых минут, он услышал знакомый голос на линии.

Джонни сказал ему: «не говори ничего, пока я не объясню тебе, что я задумал». Он рассказал все предисловие так, чтобы казалось, будто Джонни обсуждает, куда он хочет доставить вещи. Потом он сказал: «если ты сможешь добраться до телефона офиса общественных защитников сегодня днем — не отвечай. А если не сможешь, назови время, когда ты сможешь быть там». Гондорфф не ответил. Джонни продолжил: «Хорошо. Будь там в час. Я тебе позвоню. Подними трубку. Если он начнет звонить в Офис Общественных Защитников, нажимай на сброс каждые 20 секунд. Не переставай пробовать, пока не услышишь меня на другом конце».

В час дня, когда Гондорфф поднял трубку, Джонни уже ждал его. У них была живая, приятная, неторопливая беседа, начавшая серию подобных звонков, чтобы спланировать аферу, которая принесет деньги на оплату легальных счетов — свободных от правительственной завесы.

### **Анализ обмана**

Этот эпизод показывает основной пример того, как социальный инженер может сделать то, что кажется невозможным, обманывая нескольких людей, каждый из которых делает нечто, кажущееся непоследовательным. На самом деле, каждое действие дает маленький кусочек головоломки, пока афера не закончена.

Первая сотрудница телефонной компании думала, что отдает информацию из гособслуживания.

Следующая сотрудница телефонной компании знала, что она не должна изменять класс линии без соответствующего приказа, но все равно помогла дружелюбному мужчине. Это дало возможность звонить во все 10 отделений тюрьмы.

Для мужчины из исправительной колонии в Майами, просьба помочь другому федеральному учреждению, у которого проблемы с компьютером, звучала абсолютно убедительной. И даже если у него не было другой причины узнать номер отделения, почему бы не ответить на вопрос?

А охранник в Северном-10, поверивший, что собеседник действительно из этого же заведения, звонит по официальному делу? Это была полностью приемлемая просьба, так что он позвал заключенного Гондорффа к телефону. Совсем не серьезное дело.

Серия хорошо спланированных рассказов, которые складываются в единую цепь.

## Легкие деньги

Когда а впервые познакомился с компьютерами в старших классах школы, нам приходилось подключаться к одному центральному миникомпьютеру DEC PDP 11, расположенному в пригороде Лос-Анджелеса, который использовали все школы Л.А. Операционная система на компьютере называлась RSTS/E, и эта была первая операционная система, с которой я научился работать.

В то время, в 1981 году, DEC устраивали ежегодную конференцию для своих пользователей, и в этом году конференция пройдет в Л.А. В популярном журнале для пользователей этой операционной системы было объявление о новой разработке по безопасности, Lock-11. Этот продукт продвигали с хорошей рекламной кампанией, где говорилось нечто вроде: «Сейчас 3:30 утра, и Джонни с другого конца улицы нашел ваш номер дозвона, 555-0336, с 336й попытки. Он внутри, а вы в полете. Покупайте Lock-11». Продукт, как говорилось в рекламе, был «хакероустойчивым». И его собирались показать на конференции.

Я жаждал посмотреть на разработку. Друг старшекласник, Винни, являвшийся моим партнером по хакингу в течение нескольких лет, впоследствии ставший государственным информатором против меня, разделял мой интерес к новому продукту DEC, и воодушевил меня на поход на конференцию с ним.

### Деньги на линии

Мы пришли и обнаружили большой переполох в толпе около презентации Lock-11. Похоже, что разработчики ставили деньги на то, что никто не сможет взломать их продукт. Звучит как вызов, перед которым я не смог устоять. Мы направились прямо к стенду Lock-11, и обнаружили, что руководят там разработчики проекта; я узнал их, и они узнали меня — даже в юности у меня уже была репутация фрикера и хакера из-за большого рассказа в *LA Times* о моем первом контакте с властями. В статье рассказывалось, как я благодаря одним диалогам вошел посреди ночи в здание Pacific Telephone (телефонная компания — прим. переводчика), и вышел с компьютерными руководствами, прямо перед носом у их охраны. ( Похоже, что *Times* хотели напечатать сенсационный рассказ, и в своих целях напечатали мое имя; я был еще несовершеннолетним, и статья нарушала не только традиции, а возможно даже закон о сокрытии имен несовершеннолетних, обвиненных в правонарушении.)

Когда Винни и я подошли, это вызвало интерес у обеих сторон. С их стороны был интерес, потому что они узнали во мне хакера, о котором читали, и были

немного шокированы, увидав меня. Интерес с нашей стороны вызвало то, что у каждого из трех разработчиков, стоявших там, был чек на \$100, торчавший из значка участника конференции. В сумме приз для любого, кто сможет взломать их систему, составлял \$300 — и это показалось большой суммой денег для пары тинэйджеров. Мы с трудом могли дождаться того, чтобы начать.

Lock-11 был спроектирован по признанному принципу, полагавшемуся на два уровня безопасности. У пользователя должен был быть верный идентификационный номер и пароль, но и вдобавок этот идентификационный номер и пароль будут работать, только если они введены с уполномоченного терминала, подход называемый *terminal-based security* (безопасность, основанная на терминалах) . Чтобы победить систему, хакеру бы понадобилось не только знание идентификационного номера и пароля, но и пришлось бы ввести информацию с правильного компьютера. Метод был хорошо признанным, и изобретатели Lock-11 были убеждены, что он будет держать плохих парней подальше. Мы решили преподать им урок, и заработать триста баксов.

Знакомый парень, который считался гуру в RSTS/E, уже подошел к стенду раньше нас. Несколько лет назад, он был одним из тех парней, кто озадачил меня взломом внутреннего компьютера разработчиков DEC, после чего его сообщники выдали меня. Теперь он стал уважаемым программистом. Мы узнали, что он пытался взломать программу безопасности Lock-11, незадолго до того, как мы пришли, но не смог. Этот инцидент дал разработчикам еще большую уверенность, что их продукт действительно безопасен.

Соревнование было непосредственным испытанием: ты взламываешь — ты получаешь деньги. Хороший публичный трюк ... если кто-нибудь не опозорит их и заберет деньги. Они были так уверены в своей разработке, и были достаточно наглыми, что даже приклеили распечатку на стенд с номерами учетных записей и соответствующих паролей в системе. Но не только пользовательские учетные записи, но и все привилегированные.

Это было гораздо менее приятно, чем звучит. С таким видом настроек, я знал, что каждый терминал подключен к порту на самом компьютере. Это — не ракетная физика, чтобы догадаться, что они установили пять терминалов в зале для конференций, и посетитель мог войти только как непривилегированный пользователь — это значит, что подключения были возможны только с учетных записей с правами системного администратора. Похоже, что было только два пути: обойти систему безопасности, для предотвращения чего и был рассчитан Lock-11, или как-нибудь обойти программное обеспечение, как разработчики даже не представляли.

**Terminal-based security** — Безопасность, частично основанная на идентификации конкретного используемого компьютера; этот метод был особо популярен с главными компьютерами IBM.

### **Вызов принят**

Мы с Винни уходили и говорили о конкурсе, и я придумал план. Мы невинно ходили вокруг, поглядывая на стенд с расстояния. Во время обеда, когда толпа разошлась, и трое разработчиков решили воспользоваться перерывом и пошли вместе купить себе что-нибудь поесть, оставив женщину, которая могла быть женой или девушкой одного из них. Мы прогуливались туда-сюда, и я отвлекал женщину, разговаривал с ней о разных вещах: «давно ли ты работаешь в компании?», «какие еще продукты вашей компании имеются в продаже» и т.д.

Тем временем, Винни, вне поля ее зрения, приступил к работе, используя навыки, которые мы развивали. Помимо очарованности взломом компьютеров и моего интереса к магии, мы были заинтересованы в обучении открытия замков. Когда я был маленьким, я прочесывал полки подпольного книжного магазина в Сан-Франциско, в котором были тома о вскрытии замков, вылезании из наручников, создании поддельных удостоверений — и о других вещах, о которых дети не должны знать. Винни, как и я, тренировался вскрывать замки до тех пор, пока у нас не стало хорошо получаться с замками магазинов с железом. Было время, когда я устраивал розыгрыши — находил кого-нибудь, кто использовал 2 замка для безопасности, вскрывал их и менял местами, и это очень удивляло и расстраивало, если он пытался открыть их не тем ключом.

В выставочном зале, я продолжал отвлекать девушку, пока Винни подполз сзади будки, вскрыл замок в кабинет, где стоял их PDP-11 и кабели. Назвать кабинет запертым — это почти шутка. Он был защищен тем, что слесари называют wafer lock (вафельный замок), известный как легко открываемый, даже для таких неуклюжих любителей взламывать замки как мы.

Винни понадобилась примерно минута, чтобы открыть замок. Внутри, в кабинете он обнаружил то, что мы не любили: полосы портов, для подключения пользовательских терминалов, и один порт, который называется консольным терминалом. Этот терминал использовался оператором или системным администратором, чтобы управлять всеми компьютерами. Винни подключил кабель, идущий от консольного порта к одному из терминалов, находящихся на выставке.

Это означало, что теперь этот терминал воспринимается как консольный терминал. Я сел за переподключенную машину, и использовал пароль, который так смело предоставили разработчики. Поскольку Lock-11 определил, что я подключаюсь с уполномоченного терминала, он дал мне доступ, и я был подключен с правами системного администратора. Я

пропатчил операционную систему, изменил ее так, что можно будет подключиться с любого компьютера на этаже в качестве привилегированного пользователя.

Когда я установил свой секретный патч, Винни вернулся к работе, отключил терминальный кабель и подключил его туда, где он был первоначально. Он еще раз вскрыл замок, на этот раз, чтобы закрыть дверь кабинета.

Я сделал листинг директорий, в поисках папок и программ, связанных с Lock-11, и случайно наткнулся на кое-что шокирующее: директория, которая не должна была быть на этой машине. Разработчики были слишком уверены, что их программное обеспечение непобедимо, что они даже не побеспокоились о том, чтобы убрать исходный код их нового продукта. Я передвинулся к соседнему печатающему терминалу, и начал распечатывать порции исходного кода на длинных листах зелено-полосатой бумаги, используемой компьютерами в те времена.

Винни едва успел закрыть замок и вернуться ко мне, когда парни вернулись с обеда. Они застали меня, сидящего возле компьютера бьющего по клавишам, а принтер продолжал печатать. «Что делаешь, Кевин?» — спросил один из них.

"А, просто печатаю исходники, " я сказал. Они предположили, что я шучу. Пока не посмотрели на принтер и не увидели, что это *действительно* тот ревностно охраняемый исходный код их продукта.

Они не поверили, что я действительно подключился как привилегированный пользователь. «Нажми Control-T,» — приказал один из разработчиков. Я нажал. Надпись на экране подтвердила мое утверждение. Парень ударил рукой по своему лбу, когда Винни говорил «Триста долларов, пожалуйста».

### **Сообщение от Hacker Place**

Вот еще один пример того, как умные люди недооценивают противника. А как насчет вас — вы уверены, что можно поставить \$300 на ваши охранные системы, против взломщика? Иногда обход вокруг технологических устройств не такой, какой вы ожидаете.

Они заплатили. Мы с Винни ходили по выставке оставшуюся часть дня со столларовыми чеками, прикрепленными к нашим значкам конференции. Каждый, что видел чеки, знал, что они означают.

Конечно, мы с Винни не победили их программу, и если разработчики установили бы хорошие правила в конкурсе или использовали бы действительно безопасный замок, или присматривали за своим оборудованием более внимательно, то им бы не пришлось терпеть унижение того дня — унижение из-за парочки подростков.

Позже, я узнал, что команде разработчиков пришлось зайти в банк, чтобы получить наличные: эти столларовые чеки — все деньги, взятые с собой, которые они собирались тратить.

## УМНЫЕ МОШЕННИКИ

Теперь вы выяснили, что когда незнакомец звонит с запросом на чувствительную информацию или на что-то, что может представлять ценность для атакующего, человек, принимающий звонок, должен быть обучен требовать телефонный номер вызывающего и перезванивать чтобы проверить, что человек на самом деле есть тот, за кого себя выдает — сотрудник компании, или сотрудник партнера по бизнесу, или представитель службы технической поддержки от одного из ваших поставщиков, например. Даже когда компания установила процедуру, которой сотрудники тщательно следуют для проверки звонящих, сообразительные атакующие все еще способны использовать набор трюков для обмана своих жертв, заставляя поверить что они те, за кого себя выдают. Даже сознательные в отношении безопасности сотрудники могут стать обманутыми методами, такими как нижеприведенные.

### Несоответствующий “Caller ID”

Любой кто хоть раз получал звонок на сотовой телефон, наблюдал в действии опцию, называемую “caller ID” (дословно “Идентификатор Вызывающего”) — этот знакомый дисплей, отображающий телефонный номер звонящего. В рабочей обстановке эта функция предлагает возможность рабочему одним взглядом оценить, от знакомого ли сотрудника идет вызов или же откуда-то вне компании.

Много лет назад некие амбициозные телефонные фризеры обнаружили для себя все прелести caller ID еще даже до того как телефонная компания публично стала предлагать подобный сервис абонентам. Они изрядно повесилились, одурачивая людей ответами по телефону и приветствуя вызывающего по имени, в то время как тот даже не успевал сказать ни слова. Просто когда вы думаете что подобное безопасно, практика удостоверения личности путем доверия тому что вы видите — то, что появляется на дисплее caller ID — это именно то, на что атакующий может рассчитывать.

#### **Звонок Линды**

**День/время:** Вторник, 23 июля, 15:12

**Место:** “Офисы Финансового Отдела, Авиакомпания Starbeat”

Телефон Линды Хилл зазвонил когда она записывала заметку для босса. Она взглянула на дисплей caller ID, который показывал что звонок исходил из офиса корпорации в Нью Йорке, но от кого-то по имени Виктор Мартин — имя она не узнала.

Она подумала дождаться пока звонок переключится на автоответчик, так что ей не придется отрываться от мысли заметки. Но любопытство взяло верх. Она подняла трубку и звонящий представился и сказал что он из отдела рекламы и работает над некоторым материалом для управляющего компании. “Он на пути к деловой встрече в Бостоне с кем-то из банкиров. Ему требуется первоклассный финансовый отчет на текущий квартал,” сказал он. “И еще одна вещь. Еще ему нужны финансовые прогнозы на проект Апачи,” добавил Виктор, используя кодовое название продукта, который был одним из главных релизов этой весной.

Она попросила его электронный адрес, но он сказал что у него проблема с получением электронной почты и над этим работает служба технической поддержки, поэтому не могла бы она использовать факс взамен? Она сказала что это тоже подойдет, и он дал дополнительный внутренний код для его факс-машины.

Она отослала факс несколькими минутами позже.

Но Виктор не работал в отделе рекламы. К слову сказать, он даже в компании-то не работал.

### **История Джека**

Джек Доукинс начал свою “профессиональную” карьеру в раннем возрасте в качестве карманного вора, промышляя на спортивных играх на стадионе команды Янки в оживленных помещениях под трибунами и среди ночной толпы туристов на Таймс-Скуэйр. Он так проворно и искусно доказывал что мог снять часы с запястья человека, так что тот даже не узнает. Но в его трудные подростковые годы он рос неуклюжим и не был неуловим. В компании Джувенил Холл(дворец молодежи?) Джек обучился новому ремеслу с куда меньшим риском быть схваченным.

Его текущее назначение взывало его получать информацию о квартальном доходе, издержках и финансовом потоке компании до того как эти данные подавались в Комиссию по Обмену и Ценным Бумагам и обнародовались. Его клиентом был дантист, который не хотел объяснять почему он хотел получить информацию. Предусмотрительность этого человека показалась Джеку смехотворной. Подобное он видел и до этого — у парня наверное была проблема с азартными играми, или может недешево обходящаяся любовница, о которой его жена была еще не в курсе. Или может быть он просто хвастался своей жене насчет того, как он умен на фондовой бирже; теперь же он потерял пару пакетов акций и хотел сделать нехилое вложение в нечто более надежное, зная как именно биржевая стоимость компании будет прогрессировать когда они анонсируют квартальные итоги.

Люди удивляются когда обнаруживают как мало времени требуется социальному инженеру чтобы выяснить как контролировать ситуацию, с которой он прежде никогда не сталкивался. К тому времени как Джек вернулся домой с его встречи с дантистом, у него уже сформировался план.

Его друг Чарльз Бэйтс работал в компании Панда Импорт, у которой был свой собственный телефонный коммутатор, или PBX.

В терминах, близких людям, знающим телефонные системы, PBX был подключен к цифровой телефонной службе известной как T1, сконфигурированной как Интерфейс Основного Тарифного плана цифровой сети интегрированных услуг (Primary Rate Interface ISDN(integrated services digital network), PRI ISDN — выделенный канал). Под этим подразумевается, что каждый раз когда звонок исходил от Панда Импорт, установки и другая информация обработки вызова попадали из канала данных в телефонный коммутатор компании; информация включала в себя номер вызывающей стороны, который(если не заблокирован) передавался в устройство caller ID на конце линии получателя.

Друг Джека знал как запрограммировать коммутатор так, чтобы человек, получающий вызов, видел бы на его caller ID-дисплее не действительный телефонный номер в офисе Панда Импорт, а какой угодно другой номер, который он запрограммировал в коммутатор. Этот трюк работает, поскольку местные телефонные компании не беспокоятся о подтверждении номера вызывающего, полученного от абонента, и сравнении его с действительными телефонными номерами за которые абонент платит.

Все что Джеку Доукинсу было нужно — это доступ к любому такому телефонному сервису. К счастью, его друг и временами партнер по преступлениям, Чарльз Бэйтс, всегда был рад протянуть руку помощи за соответствующее вознаграждение. В данном случае, Джек и Чарльз временно перепрограммировали телефонный коммутатор так, что звонки с конкретной телефонной линии, проходящей в зданиях Панда Импорт, подменяли бы внутренний телефонный номер Виктора Мартина, делая похожим что вызов идет из авиакомпании Starbeat.

Идея того, что ваш caller ID может быть изменен для отображения любого желаемого вами номера, так малоизвестна, что редко ставится под вопрос. В данном случае, Линда была счастлива отправить факсом запрошенную информацию парню, который, как она думала, был из рекламного отдела. Когда Джек повесил трубку, Чарльз перепрограммировал телефонный коммутатор компании, вернув телефонный номер к исходным установкам.

### **Анализ обмана**

Некоторые компании не хотят чтобы их клиенты или поставщики знали телефонные номера их сотрудников. Например, в компании Ford могут решить, что звонки из их Центра Службы Поддержки Потребителей должны отображать номер 800 для Центра и имя вроде “Поддержка Ford” вместо реального прямого телефонного номера каждого представителя службы поддержки, осуществляющего звонок. Microsoft может захотеть дать своим сотрудникам возможность говорить людям свой телефонный номер вместо того, чтобы каждый, кому они звонят, кидал взгляд на их caller ID и знал их



дополнительный код. Таким способом компания способна поддерживать конфиденциальность внутренних номеров.

Но эта же самая возможность перепрограммирования предоставляет удобную тактику для хулигана, коллекционера счетов, телемаркетолога, и, конечно же, социального инженера.

### **Знание об информационной безопасности и тренировки**

Социальный инженер задумал заполучить проект (исходники) Вашего нового продукта за 2 месяца до релиза.

Что остановит его?

Ваш файервол? Нет.

Мощная система идентификации? Нет.

Система обнаружения вторжений? Нет.

Шифрование данных? Нет.

Ограничение доступа к номерам дозвона модемов? Нет.

Кодовые имена серверов, которые затрудняют определение местонахождения проекта искомого продукта? Нет.

Смысл здесь в том, что никакая технология в мире не сможет противостоять атаке социального инженера.

### **Обеспечение безопасности с помощью технологии, тренировки и процедуры**

Компании, которые проводят тесты на возможность проникновения, сообщают, что их попытки проникнуть в компьютерную систему компании с помощью методов социнженерии практически в *100% случаев* удаются.

Технологии безопасности могут усложнить этот тип атак путем исключения людей из процесса принятия решений. Тем не менее истинно эффективный путь ослабить угрозу социальной инженерии можно через использование технологий безопасности, комбинированных с политикой безопасности, которая устанавливает правила поведения служащих, а также *включающих* обучение и тренировку сотрудников.

Единственный путь сохранить разработки Вашего продукта нетронутыми — иметь тренированную, знающую и добросовестную рабочую команду. Это подразумевает тренировку с использованием политик и процедур, но, вероятно, более важным является переход к программе распределенной осведомленности. Некоторые компании, занимающиеся вопросами безопасности, рекомендуют тратить на тренировку таких программ до 40% бюджета компании.

Первый шаг — приучить каждого на предприятии к мысли, что существуют бессовестные люди, которые могут с помощью обмана и психологии манипулировать ими. Служащие должны знать, какая информация нуждается в защите, и как эту защиту осуществлять. Однажды хорошо прочувствовав и поняв, как можно поддаться чужим манипуляциям, они будут находиться в намного более выгодной позиции, чтобы распознать атаку.

Осведомление о безопасности включает также обучение каждого работающего в компании политикам и процедурам. Как обсуждается в главе 17, политики — это необходимые и обязательные правила, которые описывают поведение сотрудников для защиты корпоративной информационной системы и особо ценной информации.

Эта и следующие главы показывают безопасный шаблон (blueprint — синька, светокопия), который обезопасит Вас от атак, которые дорого могут Вам обойтись. Если Вы не тренируете персонал, следующий процедурам обработки информации (well— thought —out procedures), это до *того* момента, *пока* Вы не потеряете информацию благодаря социальному инженеру. Не тратьте время, ожидая атак, которые могут случиться, пока решаете, разрабатывать или не разрабатывать политики безопасности: они могут разорить Ваш бизнес и разрушить благополучие Ваших рабочих.

### **Понимание того, как атакующий может воспользоваться человеческой природой**

Для того, чтобы разработать действенную программу обучения, Вы должны понять, почему люди в первую очередь уязвимы для атак. Для выделения этих тенденций в вашей программе, например, обратить на них внимание благодаря дискуссии — этим Вы поможете сотрудникам понять, как социальный инженер может манипулировать людьми.

Манипуляция начала изучаться социальными исследователями в последние 50 лет. Robert B. Cialdini, написавший в «Американской науке» (Февраль 2001), объединил результаты этих исследований и выделил 6 «черт человеческой натуры», которые используются в попытке получения нужного ответа.

Это 6 приемов, которые применяются социальными инженерами наиболее часто и успешно в попытках манипулировать.

#### **Авторитетность**

Людям свойственно желание услужить (удовлетворить запрос) человеку с авторитетом (властью). Как говорилось раньше, человек получит нужный

ответ, если сотрудник уверен, что спрашивающий имеет власть или право задавать этот вопрос.

В своей книге «Влияние» Dr. Cialdini написал об обучении в 3 госпиталях Мидвестерна, в которых аппараты 22 медсестер соединялись с человеком, который выдавал себя за физиотерапевта, инструктируя административный персонал на выписку рецепта препарата (наркотика?) пациенту. Медсестры, которые получили это указание, не знали звонившего. Они не знали, действительно ли он доктор (а он им не был). Они получали инструкции для выписки рецепта по телефону, что нарушает политику безопасности госпиталя. Препарат, который указывался, не разрешен к применению, а его доза составляла в 2 раза большую, чем допустимая суточная норма — все это может опасно отразиться на состоянии здоровья пациента или даже убить его. Более чем в 95% случаев Cialdini сообщает, что «медсестра брала необходимую дозу из палаты с медикаментами и уже была на пути к палате указанного пациента», где перехватывалась наблюдателем, который сообщал ей об эксперименте.

#### **Примеры атак:**

Социнженер пытается выдать себя за авторитетное лицо из IT департамента или должностное лицо, выполняющее задание компании.

#### **Умение расположить к себе**

Люди имеют привычку удовлетворить запрос располагающего к себе человека, или человека со сходными интересами, мнением, взглядами, либо бедами и проблемами.

#### **Примеры атак:**

В разговоре атакующий пытается выяснить увлечения и интересы жертвы, а потом с энтузиазмом сообщает, что все это ему близко. Также он может сообщить, что он из той же школы, места, или что-то похожее. Социальный инженер может даже подражать цели, чтобы создать сходство, видимую общность.

#### **Взаимность**

Мы можем машинально ответить на вопрос, когда получаем что-то взамен. Подарком в этом случае может служить материальная вещь, совет или помощь. Когда кто-то делает что-то для нас, мы чувствуем желание отплатить. Эта сильная черта человеческой натуры проявляется тогда, когда получивший подарок не ждал (не просил) его. Один из самых эффективных путей повлиять на людей, чтобы получить благосклонность (расположить к себе, а, следовательно, получить информацию) — преподнести неявно обязывающий подарок.

Поклонники религиозного культа Хари Кришны очень опытные в умении получать влияние над человеком путем преподнесения подарка — книги или цветка. Если человек пробует вернуть, отказаться от подарка, дарящий мягко

настаивает: «Это наш подарок Вам». Этот основной принцип взаимности использовался Кришнами для постоянного увеличения пожертвований.

#### **Примеры атак:**

Сотрудник получает звонок от человека, который называет себя сотрудником IT департамента. Звонящий рассказывает, что некоторые компьютеры компании заражены новым вирусом, который не обнаруживается антивирусом. Этот вирус может уничтожить (повредить) все файлы на компьютере. Звонящий предлагает поделиться информацией, как решить проблему. Затем он просит сотрудника протестировать недавно обновленную утилиту, позволяющую пользователю сменить пароли. Служащему неудобно отказать, потому что звонящий лишь предлагает помощь, которая защитит пользователей от вируса. Он хочет отплатить, сделав что-нибудь для «доброго человека». Например, ответить на пару вопросов...

#### **Ответственность**

Люди имеют привычку исполнять обещанное. Раз пообещав, мы сделаем все, потому что не хотим казаться не заслуживающими доверия. Мы будем стремиться преодолеть любые препятствия для того, чтобы сдержать слово или выполнить обязанность.

#### **Примеры атак:**

Атакующий связывается с подходящим новым сотрудником и советует ознакомиться с соглашением о политиках безопасности и процедурах, потому что это — основной закон, благодаря которому можно пользоваться информационными системами компании. После обсуждения нескольких положений о безопасности атакующий просит пароль сотрудника «для подтверждения согласия» с соглашением. Он должен быть сложным для угадывания. Когда пользователь выдает свой пароль, звонящий дает рекомендации, как выбирать пароли в следующий раз, чтоб взломщикам было сложно подобрать их. Жертва соглашается следовать советам, потому что это соответствует политике компании. К тому же рабочий предполагает, что звонивший только что подтвердил его согласие следовать соглашению.

#### **Социальная принадлежность к авторизованным**

Людям свойственно не выделяться в своей социальной группе. Действия других являются гарантом истинности в вопросе поведения. Иначе говоря, «если так делают другие, я тоже должен действовать так».

#### **Примеры атак:**

Звонящий говорит, что он проверяющий и называет имена других людей из департамента, которые занимаются проверкой вместе с ним. Жертва верит, потому что остальные названные имена принадлежат работникам департамента. Затем атакующий может задавать любые вопросы, вплоть до того, какие логин и пароль использует жертва.

#### **Ограниченное количество «бесплатного сыра»**

Еще одна из потенциально опасных для безопасности информации человеческих черт — вера в то, что объект делится частью информации, на которую претендуют другие, или что эта информация доступна только в этот момент.

### **Примеры атак:**

Атакующий рассылает электронные письма, сообщающие, что первые 500 зарегистрировавшихся на новом сайте компании выиграют 3 билета на премьеру отличного фильма. Когда ничего не подозревающий сотрудник регистрируется на сайте, его просят ввести свой адрес электронного почтового ящика на рабочем месте и выбрать пароль. Многие люди, чтоб не забыть множество паролей, часто используют один и тот же во всех системах. Воспользовавшись этим, атакующий может попытаться получить доступ к целевому рабочему или домашнему компьютеру зарегистрировавшегося.

### **Типичные методы действий социальных инженеров**




- Представляться другом-сотрудником
- Представляться сотрудником поставщика, партнерской компании, представителем закона
- Представляться кем-либо из руководства
- Представляться новым сотрудником, просящим о помощи
- Представляться поставщиком или производителем операционных систем, звонящим, чтобы предложить обновление или патч.
- Предлагать помощь в случае возникновения проблемы, потом заставить эту проблему возникнуть, принуждая жертву попросить о помощи
- Отправлять бесплатное ПО или патч жертве для установки
- Отправлять вирус или троянского коня в качестве приложения к письму
- Использование фальшивого поп-ап окна, с просьбой аутентифицироваться еще раз, или ввести пароль
- Записывание вводимых жертвой клавиш компьютером или программой
- Оставлять диск или дискету на столе у жертвы с вредоносным ПО
- Использование внутреннего сленга и терминологии для возникновения доверия
- Предлагать приз за регистрацию на сайте с именем пользователя и паролем
- Подбрасывать документ или папку в почтовый отдел компании для внутренней доставки
- Модифицирование надписи на факсе, чтобы казалось, что он пришел из компании

- Просить секретаршу принять, а потом отослать факс
- Просить отослать документ в место, которое кажется локальным
- Получение голосовой почты, чтобы работники, решившие перезвонить, подумали, что атакующий — их сотрудник
- Притворяться, что он из удаленного офиса и просит локального доступа к почте.

### **Факторы, делающие компанию более уязвимой к атакам**

- ✓ Большое количество работников
- ✓ Множество филиалов
- ✓ Информация о местонахождении сотрудников на автоответчике
- ✓ Информация о внутренних телефонах общедоступна
- ✓ Поверхностное обучение правилам безопасности
- ✓ Отсутствие системы классификации информации
- ✓ Отсутствие системы сообщения об инцидентах

### **Классификация информации**

-  **КЛАССИФИКАЦИЯ**
-  **ОПИСАНИЕ**
-  **ПРОЦЕДУРА**

- **Публичная**

Может быть свободно доступна для общественного пользования.

Не требует подтверждения личности

- **Внутренняя**

Для использования внутри компании

Проверьте, является ли просящий сотрудником в данный момент, подписал ли он соглашение о неразглашении, и попросите разрешение руководства для людей, не являющихся сотрудниками.

- **Личная**

Информация личного характера,  
предназначенная для использования только внутри организации.  
Проверьте, является ли просителя сотрудником в данный момент, или у него  
есть разрешение. Свяжитесь с отделом кадров насчет раскрытия  
информации сотрудникам или людям, не являющимся сотрудниками.

- **Конфиденциальная**

Известна только людям, которым необходимо это знать внутри организации.  
Подтвердите личность звонящего и спросите у владельца, надо ли  
звонящему это знать. Отпускайте только с письменным разрешением  
менеджера, владельца или создателя. Убедитесь, что просителя подписал  
договор о неразглашении тайн. Только менеджеры могут сообщать что-либо  
людям, не работающим в фирме.