**Социальная инженерия: как спасти компьютер от человека?**

Сегодня хотелось бы поговорить немного о компьютерной безопасности. Но не о шифровании данных, фаерволах или методах криптографии – все это сфера специалистов весьма узкой специализации. Мы же попытаемся немного разобраться с таким понятием, как социальная инженерия.

Этот термин охватывает пресловутый человеческий фактор, который приводит к возникновению катастроф даже при самой отлаженной и защищенной компьютерной системе. Даже лучший администратор по безопасности не может быть уверенным, что рядовой менеджер не окажется виновным в хищении данных, попавшись на уловку злоумышленников.



**Немного истории**

Несомненно, отцом социальной инженерии считается Кевин Митник. Имя это хакера практически легендарно благодаря шуму, который он смог поднять. Некоторые даже нарекли его первым и величайшим хакером всех времен.

Начинал хакер, навевающий ужас на государственные органы США, с невинной подделки проездных билетов. Кевин считал поездки на автобусе по Лос-Анджелесу более интересным времяпровождением, чем школа, но денег катастрофически не хватало. Тогда наблюдательный школьник порылся в мусорке на остановке и стал подделывать билеты для своих прогулок.



В 70-х 12 летний подросток присоединился к фрикерам, то есть звонящим бесплатно по телефону. Хорошее знание телефонных сетей позволяло Митнику своеобразно развлекаться – он мог сделать стационарный телефон таксофоном. Вы поднимаете трубку, а оператор просит вас заплатить 20 центов, чтобы начать звонок.

В самом начале 80-х Кевин взломал компьютерную сеть своей школы. Особенность всей хакерской карьеры этого человека в том, что он никак не воспользовался предоставленными возможностями ни для того, чтобы улучшить свои оценки, ни при будущих взломах для своего обогащения.

Так как хакер не зарабатывал на своих талантах, то долгое время он не мог позволить себе покупку компьютера. Поэтому он находил возможность воспользоваться компьютером всюду, где это было допустимо благодаря своим коммуникационным данным.

В дальнейшем от его нападок пострадали Пентагон, крупные разработчики программного обеспечения. Впервые он попал за решетку на 6 месяцев, когда взломал компьютерную сеть военных и в дальнейшем проблемы с законом только усугублялись. Кевин выдавал себя за студента университета, компьютерного техника в больнице Сиэтла и скрывался под чужими именами.

В 1999 Митник сдался и признал себя виновным. Прокурор хотел упрятать за решетку незадачливого хакера на два века, потому что его история наделала немало шума, но обошлось и его заключение должно было продлиться четыре года. Благодаря фонду FREE KEVIN энтузиасты собрали деньги, обеспечив в 2001 году досрочное освобождение Кевина.

Митник решил окончательно покончить с криминалом и пытается заниматься безопасностью сетей, написал несколько поучительных книг. В первую очередь он предлагает переживать не о технической защите компьютеров, а о человеке, который сидит за ним. По мнению хакера зачастую проще получить пароль у пользователя, чем пытаться осуществить взлом.

**Основные техники социальной инженерии**

*Претекстинг*  работает по заранее подготовленному сценарию. Обычно по телефону или Skype пользователя подталкивают на открытие каких-то данных или же на совершение определенных действий. Техника работает лучше, если изначально были собраны личные данные – имя, должность и другие полезные данные для разговора.

*Фишинг* предполагает, что пользователь будет обманут схожестью сайта с известной фирмой или банком. Часто для извещений используют электронные письма со ссылкой на фальшивую страницу. Наверное, все помнят волну подделок сайта Вконтакте. Или еще один прекрасный вариант фишинга:



Громкая фишинговая откака произошла в 2003 году, когда множество пользователей eBay подтвердили данные о своей кредитки, потому что их аккаунт якобы был заблокирован. Чаще всего для мошенничества используют популярные бренды, обещания выигрыша, используют ложные антивирусные программы. В последнее время нередко звонят, представляясь служащими банков или имитируя оператора call-центра.

*Троянский конь* - это программа, которая может воровать данные, изменять файлы, нарушать работу операционной системы. Часто его прячут в файлы, отправляемые по электронной почте, взломанные программы. Если вы устанавливаете взломанное ПО, что есть большой шанс, что ваш компьютер используется для DDoS-атак.

*Дорожное яблоко* – это проникновение в сеть с помощью пользователя. Какой-либо физический носитель оставляется для того, чтобы пользователь нашел и по причине любопытства подключил его к своему рабочему компьютеру. Нередко на диски наносят официальные логотипы компании.

*Кво про кво (Quid pro quo – услуга за услугу)* – этот вид мошенничества предполагает звонок по корпоративному телефону. Злоумышленник представляется службой поддержки и в процессе помощи с техническими неполадками пытается выудить полезную информацию или же запустить вредоносное программное обеспечение.

*Обратная социальная инженерия* заключается в том, что пользователь сам обращается за помощью к злоумышленнику. Многие пользователи без проблем дают свои личные данные, чтобы упростить и ускорить процесс решения проблем. Обращаясь к компьютерным специалистам, люди искренне полагаются на их порядочность. Можно самостоятельно создать проблему, чтобы помочь с ее решением. Могут присылаться сообщения о том, куда обратиться за помощью.

**Немного из жизни**

Как бы ни казалось, что методы социальной инженерии смешные, но тысячи и миллионы людей продолжают попадаться на крючок злоумышленников. Ведь действительно – сложность сетей настолько велика, что легче затратить время на подготовку атаки на пользователя.

На сайте [Хабрахабр](http://habrahabr.ru/post/89109/) есть интересная история из жизни про дорожное яблоко. Причем, диск с вирусом передался системному администратору, а не обычному пользователю. Если бы не достаточно хорошо настроенная компьютерная безопасность, то, скорее всего, метод сработал бы.

В практике моих друзей в студенческую пору было интересное развлечение. В ту полу у многих были смартфоны на базе операционной системы Symbian. Ребята запаковывали в архив с файлами популярный вирус, который не давал выключить блютуз соединение и нещадно разряжал аккумулятор. Самое патовое в ситуации, что при распаковке архива появлялся вопрос: «Архив содержит вирус. Вы точно хотите распаковать его?». Ни один человек ничего не спросил и не подумал о том, чтобы не открывать файлы.

Что говорить о простых людях, когда освещение дня принца Уильяма на службе ВВС королевства Великобритании ознаменовалось тем, что называют epic fail – просто на стене висел распечатанный лист с паролями и некоторой информацией для внутреннего использования:



Компьютерная грамотность многих пользователей на таком низком уровне, что обмануть их не составляет труда. Я лично несколько раз запускала на компьютерах друзей с флешки маленькую программку от Лаборатории Касперского (это даже не вирус), обещая проверку на редкий вирус. Причем, объяснять свои действия чаще всего и вовсе не требуется. Спустя 30 секунд у меня были все последние введенные пароли для авторизации на том или ином сайте.

Еще один интересный случай. При разработке проектов часто ставят простой и стандартный пароль. Так вот, при проверке нередко оказывается, что дефолтный пароль могут не менять в течение долгого периода времени. Не знаю, как вы, а вот я заходила в административную панель нескольких сайтов, введя магические admin admin. Даже смены регистра не понадобилось.

**Как защититься? Практические советы**

Самое печальное в социальной инженерии – это отсутствие универсальных и реально действующих мер противодействия. Человек – это самый ненадежный винтик любой компьютерной системы. Наверное, единственный способ пресечь любые атаки – это забрать у пользователя права, отключить дисковод и USB порты, Интернет соединение… а лучше и вовсе не подпускать к компьютеру ☺.

Но все-таки вы можете попробовать обезопасить вашу сеть от пользователя. Вот некоторые советы:

1. Приучите ваших сотрудников к тому, что пароль от рабочего компьютера, баз данных – это собственность компании. Точно такой же пароль не должен стоять для авторизации на личной почте, меседжерах, форумах или в социальных сетях. Один и тот же пароль на всех ресурсах – далеко не редкость. А украсть данные с домашнего ПК не составит большого труда.
2. Лучше всего, если произносить свои пароли нельзя ни по телефону, ни по Skype. Системному администратору все доступно с рабочего места. А вот злоумышленник спокойно может воспользоваться телефоном или прийти лично, как будто он новый сотрудник. Это особенно проблемно в больших компаниях, где большинство работников не знакомы друг с другом.
3. Операционная система должна быть максимально закрыта от пользователя. Лучше всего отключить возможность подключения внешних носителей информации, если в этом нет особой необходимости. Ввести строгий запрет на подключение своих носителей или тем более найденных.

Также знайте, что постоянная смена паролей не панацея – вспомните ситуацию с ВВС Великобритании. Пользователи просто повесят бумажку с данными, желательно, на самое видное место, хитрые – приклеят под клавиатуру.

Не забывайте, что один способ защиты ничем не поможет. Я видела фирму, где под страхом смертной казни запрещали подключать что-либо к USB порту, даже для подзарядки телефона. Но при этом на компьютере с важной базой данных был установлен пиратский CS 1.6 и был свободный доступ ко всему пространству Всемирной паутины.

Конечно, шпионаж и кража разработок обычно касается корпораций и больших фирм. Но фишинговые и троянские атаки зачастую направлены на любой компьютер. Да и конкуренты есть у всех. Обязательно занимайтесь образованием ваших сотрудников, а иначе в один день [пляшущие свинки](http://ru.wikipedia.org/wiki/%D0%9F%D0%BB%D1%8F%D1%88%D1%83%D1%89%D0%B8%D0%B5_%D1%81%D0%B2%D0%B8%D0%BD%D0%BA%D0%B8) могут стать причиной потери важной документации или несколько месячного проекта.



**Эксперты о социальной инженерии**

Мы решили поинтересоваться, что думают по поводу социальной инженерии крупные производители антивирусных программ для защиты данных. Нам ответил [Dr. Web](http://www.drweb.com/%22%20%5Ct%20%22_blank).
 **Не секрет, что совершенство системы защиты зачастую претерпевает сбой в тот момент, как за компьютер садится человек. Антивирусные фирмы, стараясь блокировать фишинговые сайты, вводят родительский контроль. Есть ли еще какие-то инструменты от вашей компании, которые позволяют защитить ПК от малообразованного пользователя?**

Вы знаете, один из наших сотрудников некоторое время назад придумал отличную фразу —  «Самый страшный вирус сидит перед монитором». Мы даже сделали с ней серию футболок для наших пользователей:


С одной стороны, над фразой можно посмеяться. С другой — нельзя не заметить, что она правдива. К сожалению, ни один антивирус, ни одна система безопасности не смогут защитить пользователя, который не проявляет осторожность, выходя в Интернет или пользуясь компьютером, подключенным к Интернету. Естественно, у нас представлено несколько продуктов для защиты обычных, или домашних пользователей. Для комплексной защиты мы предлагаем Dr.Web Security Space. Для базовой защиты — Антивирус Dr.Web. Также прекрасно известны и широко распространены наши бесплатные утилиты. Например, известность Dr.Web CureIt!, нашего бесплатного сканера, давно вышла за пределы России и даже Европы. А второй страной по числу пользователей нашего антивируса для Android является Япония.

**У вас в офисе наверняка должна быть хорошая защита сети. Случались ли какие-то поучительные ситуации, когда по глупости или невнимательности кто-то из сотрудников становился жертвой злоумышленника? Или у вас даже секретари — «безопасники» с 5-летним стажем?**

Будучи компанией, специализирующейся на информационной безопасности, мы естественным образом пристальное внимание уделяем защите наших данных. Впрочем, деятельность некоторых сотрудников имеет несколько другую специализацию. Для того, чтобы исключить ошибки, которые могут привести к заражениям или потере конфиденциальных данных, существуют политики безопасности. И сотрудники, которые следят за их исполнением.

**Можете ли дать какие-то советы из собственного опыта для администраторов по безопасности или же простых пользователей относительно того, как защитить компьютер от человека?**

Первое — быть бдительным. Второе — иметь обновленный антивирус (не обязательно Dr.Web — это вы решаете сами. Главное, чтобы вы использовали актуальную антивирусную защиту). Третье — обновлять не только его вирусные базы, но и модули. Иногда это происходит не автоматически. Дабы узнать, как установить, к примеру, абсолютно новую версию антивируса, которую вы используете, подпишитесь на новости компании, которая его сделала. И хотя бы иногда их читайте. Наконец, четвертое: рассказывайте о первых трех пунктах друзьям и коллегам. Неосознанно именно они могут послужить причиной вашего заражения вредоносной программой.