

Крис Касперски

СЕКРЕТНОЕ ОРУЖИЕ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

kk@sendmail.ru

Секретное оружие социальной инженерии

"Искусство рассуждать – это искусство обманывать самого себя".
Антуан де Сент-Экзюпери "Цитадель"

Введение

Даже самая совершенная система защиты бесполезна, если ею управляет психологически неустойчивый, наивный и/или доверчивый человек. Помните анекдот о диссертации на тему "зависимость скорости перебора паролей от температуры паяльника (утюга)"? Многие почему-то забывают, что в роли объекта атаки может выступать не только машина, но и ее оператор. Причем, оператор зачастую оказывается *слабейшим* звеном в системе защиты.

На хакерском жаргоне атака на человека называется *социальной инженерией* (*social engineering*) и в своем каноническом виде обычно сводится к звонкам по телефону с целью получения конфиденциальной информации (как правило, паролей) посредством выдачи себя за другое лицо.

В данной статье термин "социальная инженерия" рассматривается намного шире и обозначает любые способы психологического воздействия на человека, как то: *введение в заблуждение* (обман), *игра на чувствах* (любви, ненависти, зависти, алчности, в том числе и *шантаж*).

Собственно, подобные приемы не новы и известны еще со времен глубокой древности. Остается только удивляться тому, что за истекшие тысячелетия человечество так и не научилось противостоять мошенникам и отличать правду от лжи. Еще удивительнее то, что арсенал злоумышленников не претерпел никаких принципиальных изменений. Напротив, с развитием коммуникационных технологий их задача значительно упростилась.

Общаясь по Интернет, вы не видите и не слышите своего собеседника, более того, нет никаких гарантий, что сообщение действительно отправлено тем адресатом, имя которого стоит в заголовке. Атакующий может находиться и в соседней

комнате, и в соседнем городе, и даже на соседнем континенте! Все это значительно усложняет идентификацию личности, поиск и доказательство причастности злоумышленника к атаке. Стоит ли удивляться огромной популярности социальной инженерии среди молодежи?

К счастью, подавляющее большинство мошенников действует по идентичным или близким шаблонам. Поэтому, изучение приемов их "работы" позволяет распознать обман и не попасться на удочку. Автором этой статьи собрана обширная коллекция хакерского арсенала, наиболее популярные "экспонаты" которой представлены ниже. Конечно, на исчерпывающее руководство по обеспечению собственной безопасности данная публикация не претендует, но общее представление о методиках хищения денег и/или информации все же дает.

Введение в заблуждение (обман)

Введение в заблуждение — основной "компонент" социальной инженерии, включающий в себя целый ряд всевозможных техник: *выдача себя за другое лицо, отвлечение внимания, нагнетание психологического напряжения* и т. д. Конечные цели обмана так же весьма разнообразны. Ниже мы рассмотрим лишь наиболее популярные из них: *отъем денег, получение несанкционированного доступа к конфиденциальной информации и уход от ответственности путем перевода подозрений на постороннее лицо.*

Отъем денег. Это только в американских боевиках одетые в маски грабители вламываются в какой-нибудь банк и, угрожая оружием, требуют деньги на бочку. В России же все происходит гораздо проще. Вездесущий бардак и халатное отношение к собственным обязанностям позволяют присвоить чужую зарплату простой росписью в ведомости. Автор этой статьи был до глубины души поражен, когда обнаружил, что многие издательства выплачивают гонорары, не требуя ни паспорта, ни другого удостоверения личности! Просто заходишь в бухгалтерию, говоришь что ты за северный олень такой, царапаешь фамилию в ведомости (не обязательно свою и не обязательно ту же самую, что в прошлый раз), получаешь наличные и, забыв сказать "до свидания", уходишь.

Ситуацию серьезно осложняет то обстоятельство, что далеко не всех своих корреспондентов издатель знает в лицо, т.к. многие из них проживают в другом городе или даже стране. *Для пресечения обмана все денежные вопросы следует решать не по электронной почте, по телефону, а еще лучше — выплачивать гонорар только после заключения договора.* (Договор же можно переслать обычной почтой или, на худой конец, по факсу). Кстати, встречаются и недобросовестные авторы, которые, получив деньги, требуют их снова, мотивируя это тем, что гонорар якобы получил кто-то другой, выдавший себя за них.

Бесплатное приобретение программных продуктов. Хищение денег — это достаточно рискованный способ мошенничества и, в случае неудачи, он может обернуться лишением свободы на длительный срок. Поэтому, многие предпочитают воровать не деньги, а их материальное воплощение.

Предположим, злоумышленнику требуется некоторый программный пакет и/или техническая консультация. Взломать демо-версию или атаковать локальную сеть фирмы-разработчика? Чревато! Лучше, представившись журналистом, попросить один экземпляр программы в обмен на обещание разрекламировать ее в некотором популярном журнале. Какая фирма не клюнет на такую заманчивую перспективу? К тому же вместе с продуктом злоумышленник получит и квалифицированную техническую поддержку непосредственно от самих разработчиков, а не девушек-операторов, обслуживающих рядовых клиентов.

Если вы хотите избежать обмана — пересылайте продукт не напрямую, а через издателя. Он-то наверняка знает своих журналистов! Впрочем, вполне "всамомделешний" журналист может продукт взять, а статью не написать. Или написать, но по независящим от него причинам не сумеет ее опубликовать...

Злоумышленнику придется сложнее, если требуемый ему продукт настолько специфичен, что вообще отсутствует на рынке. Разработка "под ключ" обычно стоит дорого, очень дорого, но если проявить чуточку смекали... Вот на сайте аля www.jobs.ru появляется объявление о высокооплачиваемой работе по Интернету. Прием сотрудников, естественно, происходит на конкурсной основе и каждому кандидату дается тестовое задание, по результатам выполнения которого и судят о его, кандидата, профессионализме. Вы не прошли тест? Не расстраивайтесь! Подучитесь, а потом попробуйте свои силы снова, если, конечно, к тому времени не поймете, кто остался с носом, а кто — с готовым продуктом. Самое печальное, что предъявлять злоумышленнику гражданский иск бессмысленно, поскольку состав преступления отсутствует.

Защитить себя от подобных обманов очень трудно, поскольку, аналогичная схема набора сотрудников широко используется и легальными фирмами. Напротив, очень немногие работодатели готовы оплачивать работу "котов в мешке". Поиск хорошей работы — это вообще рулетка и без разочарований здесь не обойтись.

Несанкционированный доступ. Приемы хищения паролей. Вероятно, самый известный прием похищения пароля — это звонок жертве от имени администратора системы или, напротив, администратору — от имени некоторого пользователя. Просьба в обоих случаях одна, — под каким бы то ни было предлогом сообщить пароль на некоторый ресурс. К счастью, актуальность атак этого типа за последний год значительно снизилась — все-таки жизнь чему-то учит! Однако не стоит питать иллюзий по поводу своей защищенности. Она в большинстве случаев мнимая.

Лучший способ выведать пароль — не спрашивать его. Напротив, строго-настрого запретить говорить! Это может выглядеть, например, так: *"Ало, здравствуйте! С Вами проводит разъяснительную беседу эксперт по безопасности Вася Пупкин. Помните ли Вы, что никогда, ни при каких обстоятельствах, никому-никому не должны сообщать свой пароль? А помните, что пароль должен состоять из комбинации букв и цифр? Кстати, какой он у Вас?"* Поразительно, но многие, пропуская "разъяснительную беседу" мимо ушей, называют свой действительный пароль! Причем, атакующий в случае провала ничем не рискует, т.к. вопрос *"какой у Вас пароль"* можно понимать двояко — какой именно пароль, и какой пароль вообще (длиннее восьми символов, является ли словарным словом или нет и т.д.).

А если пользователи окажутся достаточно сообразительными для того, чтобы не сообщать свой пароль первому встречному? Тогда, учитывая, что очень многие из нас склонны назначать одинаковые пароли на все ресурсы, злоумышленник просто подsunет жертве ресурс, требующий аутентификации (например, предложит подписаться на почтовую рассылку). В крайнем случае, он узнает если не сам пароль, то хотя бы привычки жертвы — выбирает ли она в качестве паролей словарные слова, и если выбирает, то по какому принципу. Разумеется, для подобного анализа придется отследить несколько назначений паролей, но никаких подозрений жертвы (даже самой квалифицированной!) это не вызовет. *Поэтому, никогда не назначайте одинаковые или близкие пароли на различные ресурсы!*

Для низко квалифицированных пользователей припасена и другая тактика. О том, что свой пароль разглашать ни в коем случае нельзя, их, вероятнее всего, уже предупредили. Но сказали ли им: где этот пароль хранится и как его можно обойти? Злоумышленник может попросить (а от имени начальника и приказать) выполнить некоторые, вполне безобидные с точки зрения жертвы действия, например, переслать PwL файл по такому-то адресу или создать нового пользователя с пустым паролем. (Причем, выполняя по шагам расписанные действия, жертва, возможно, даже не осознает, что она вообще делает). *Помните, низко квалифицированный оператор — все равно, что обезьяна с гранатой!*

Кстати, постоянная смена паролей — это *худший* выход из ситуации, создающий проблем больше, чем их решающий. Никто не будет и пытаться запомнить длинные, постоянно меняющиеся, да к тому лишенные всякого смысла пароли! Все будут их... записывать! Никакие угрозы администратора ситуацию не исправят, а, напротив, ее усугубят. Поставьте себя на место пользователя, в заветном месте хранящего такую бумажку с паролем. А теперь вообразите, что некий "доброжелатель" из "соседнего отдела" вам звонит и сообщает, что вас ожидает тотальный обыск на предмет поиска парольных бумажек с последующим увольнением всех, у кого такая бумажка обнаружится. Не знаю, сожжете ли Вы свою бумажку или запьете ее молоком, но есть ненулевая вероятность того, что кто-то избавится от излишних его улик через окно или мусорную корзину. Злоумышленнику остается лишь хорошо порыться в мусоре или под окнами фирмы. *Поэтому, любое приказание и любая служебная инструкция должна составляться осмысленно с учетом реальной ситуации, а не теоретических измышлений. Люди — не компьютеры!*

В некоторых, не таких уж редких случаях, злоумышленник имеет принципиальную возможность подсмотреть набираемый на клавиатуре пароль (например, с помощью сильного бинокля, расположившись в соседнем здании). Самое трудное — уследить за быстро набираемым паролем, к тому же частично закрытым руками и другими частями тела. Каким либо образом инициировав смену паролей (например, путем имитации атаки), он существенно упростит свою задачу. Ведь новый пароль уже не наберешь "на автомате"!

Для предотвращения утечки информации компьютеры лучше всего располагать так, чтобы ни монитор, ни клавиатура, ни принтерные распечатки не были видны ни из окон, ни из дверей. Эти несложные меры значительно усложнят хакеру проникновение в систему.

Атака администратора системы. В том случае, если пароль заполучить не удастся, злоумышленнику ничего не останется, как прибегнуть к атаке на технические средства (т.е. непосредственно на компьютеры). Однако правильно сконфигурированную и хорошо защищенную систему ломать "в лоб" практически бесполезно. Вот если бы в ней была дыра...

Один из нетехнических способов пробивания дыр выглядит приблизительно так: злоумышленник звонит администратору и сообщает, что из достоверных источников ему стало известно о готовящейся (или уже совершенной) атаке. Никаких деталей звонящий, естественно, не сообщает (он ведь не взломщик, а "знакомый" взломщика), но приблизительное местонахождение дырки все же указывает. Существует ненулевая вероятность того, что администратор, пытаясь повысить безопасность своей системы, допустит несколько ошибок, упрощающих атаку. (И эта вероятность тем больше, чем сильнее волнуется администратор).

Для отвлечения внимания злоумышленники часто прибегают к имитации атаки, выполняя различные бессмысленные, но целенаправленные действия. Автору этой статьи известно несколько случаев, когда в ответ на мусор, направленный в 80-й порт, администраторы просто "срубали" WEB-сервисы, поскольку, будучи предупрежденными об "атаке", считали: лучше на время остаться без WEB'a, чем позволить хакерам проникнуть в локальную сеть и похитить конфиденциальную информацию. Естественно, простой WEB-серверов обернулся внушительными убытками, хотя никакой опасности на самом деле и не было. *Так что не стоит шарахаться от каждой тени и любое непонятное действие расценивать как вторжение в систему.*

Развивая идею дальше, злоумышленники догадались, что выдавать себя за знакомого злоумышленника, согласного за определенное вознаграждение быть осведомителем, гораздо выгоднее, чем атаковать систему. К тому же, "осведомителя" чрезвычайно трудно привлечь к ответственности, поскольку факт обмана практически не докажем, а имитация атаки, не влекущая несанкционированного доступа к системе (блокирования системы), вообще не наказуема. Причем, для такой "атаки" злоумышленнику не требуется практически никакой квалификации, и стать "хакером" может буквально любой! *Поэтому, не спешите оплачивать услуги осведомителя, даже если он согласен "работать" почти задаром* - сначала убедитесь, что это действительно осведомитель, и что вас действительно атакуют, а не создают лишь видимость атаки! Но не забывайте, что упускать из рук настоящего осведомителя (а такие — не редкость среди хакеров) очень глупо.

Уход от ответственности. Успешно выполнить атаку — означает решить лишь половину задачи. Злоумышленнику еще предстоит замести за собой следы — уйти от ответственности и не попасться. А это, кстати, намного сложнее! Поэтому, матерые мошенники, похитив энную сумму денег, без тени жалости переводят большую ее часть на счет одного из сотрудников фирмы, который в принципе подходит на роль похитителя. Причем, это должен быть жадный, азартный и умственно недалекий человек, который, обнаружив на своем счете "лишние" деньги, с высокой степенью вероятности рискнет прикарманить добро, само идущее к нему в руки, а не побежит в милицию. Затем следует анонимный звонок (письмо) директору фирмы с сообщением: где следует искать пропавшие деньги и... жертве будет чрезвычайно

трудно доказать, что она тут ни при чем, и убедить остальных, что ее подставили. Конечно, путь денег (кто именно перевел их жертве) проследить вполне возможно (особенно, если это крупная сумма), но, во-первых, злоумышленник может переводить деньги через подставное лицо. А, во-вторых, даже будучи пойманным, он сможет заявить, что он не главарь, а пешка и вообще не знал, что деньги ворованные. При условии, что злоумышленник оставит себе меньшую часть награбленного, такая легенда будет звучать весьма убедительно. Поэтому, при "разборе полетов" ни в коем случае не хватайте первого попавшегося под руку обвиняемого — в большинстве случаев он действительно ни в чем не виновен.

Другой способ "перевода стрелок" заключается в психологической обработке лиц, "помешанных" на подражательстве хакерам, но хакерами не являющимися. Сначала их убеждают, что пребывание в тюрьме — явление вполне нормальное для хакера, затем демонстрируют целую серию эффективных "взломов", чем вызывают глубокое уважение к себе. Наконец, когда "клиент" готов, мошенник предлагает ему стать своим учеником, после чего руками ученика осуществляет реальный взлом. В случае раскрытия преступления ученик может и не выдать своего "наставника" (а при правильной психологической обработке и не выдаст, хоть режь его на куски). А, если даже и выдаст, следствию будет не так-то легко уличить злоумышленника, ведь все предыдущие атаки — фикция! "Наставник" без больших трудов сможет представить все это невинной игрой. Он-де, просто забавлялся, не причиняя никому никакого вреда. А о том, кто руководил "учеником" в настоящей атаке, — не имеет ни малейшего представления.

Впрочем, заставить ученика молчать можно и другими способами, тем же шантажом, скажем, но об этом позже.

Маска, я тебя знаю или как злоумышленники выдают себя за другое лицо.

Электронная почта, конечно, штука хорошая, но слишком уж небезопасная. Неудивительно, что многие из нас предпочитают все более или менее важные дела решать по телефону (так, по крайней мере, слышен хотя бы голос собеседника). Злоумышленника, выдающего себя за другое лицо, могут серьезно озадачить просьбой оставить свой телефон. Конечно, можно просто подключиться к "лапше" на лестничной площадке или прибегнуть к помощи таксофона (многие таксофоны умеют принимать и входящие звонки). Однако существуют и более изощренные приемы. Рассмотрим два, наиболее популярных, из них.

Захват телефона. Допустим, злоумышленник выдает себя за сотрудника такой-то компании. В телефонном справочнике он находит телефон секретаря этой компании и просит соединить его с охранником, а заодно — сообщить его телефонный номер (зачем — мошеннику придумать большого труда не составит). Если охранник действительно имеет телефон (а, что, встречаются охранники без телефона?), разыгрывается следующая комбинация. Дав жертве телефон секретаря фирмы, и, сообщив "добавочный" охранника (но, умолчав, что это — охранник), злоумышленник под каким-либо предлогом просит жертву позвонить ему в строго определенное время. Незадолго до назначенного срока злоумышленник заходит в фирму, где и встречается с охранником, сидящим у входа. Рассказав какую-нибудь душещипательную историю (типа по ошибке дал своему партеру по бизнесу ваш телефон),

злоумышленник спрашивает: а вот сейчас, когда позвонят и попросят "Васю", нельзя ли будет ему взять трубочку? Поскольку, с точки зрения охранника никакого криминала в этом нет, существует определенная вероятность того, что он исполнит эту просьбу (особенно, если злоумышленник — девушка привлекательной наружности). В результате, жертва будет считать, что злоумышленник действительно работает в этой фирме.

В качестве альтернативного варианта злоумышленник может попросить охранника сказать звонящему: "*Перезвоните Васе по такому-то телефону*". Если охранник не будет вдаваться в подробности, жертва опять-таки подумает, что, раз Васю знают, то он, несомненно, подлинный сотрудник этой фирмы. Конечно, охранник может запомнить внешность злоумышленника (и запомнит наверняка, если он профессионал), но внешность — это не паспортные данные и мошенника еще предстоит найти. К тому же, личная встреча с охранником абсолютно необязательна. Злоумышленник может позвонить по любому телефону и попросить его владельца сообщить звонящему по какому телефону можно найти Васю. Практика показывает, что люди (особенно занятые) редко вдаются в подробности и вместо того, чтобы сказать: "*Ах, Вам Васю? А Вася здесь не работает! Он, знаете ли, наш телефон дал Вам по ошибке...*" ограничиваются кратким: "*Васю? Позвоните по такому-то телефону*".

Поэтому, ни в коем случае не стоит считать телефон надежным средством идентификации личности.

Место встречи изменить нельзя. В некоторых случаях возможностей телефонных и компьютерных сетей оказывается недостаточно и злоумышленнику приходится прибегать к встречам "в живую". Как убедительно выдать себя за другое лицо, да так, чтобы у жертвы не возникло и тени сомнения? Ведь, в противном случае она запросто может попросить предъявить документы, а качественно подделать документы очень сложно (во всяком случае, для одиночки).

Допустим, злоумышленник выдает себя за сотрудника некоторой фирмы и, чтобы вы окончательно поверили в это, договаривается встретиться с вами в здании фирмы. Чтобы не возиться с выписыванием пропусков, он предлагает подождать вас на проходной. Для усиления эффекта проходящие мимо "сотрудники" могут здороваться со злоумышленником и жать ему руку. Зима, кстати, лучший помощник злоумышленника. Сняв верхнюю одежду и спрятав ее, например, в припаркованной рядом машине, он окончательно развеет ваши сомнения относительно его личности.

Техника проникновения на охраняемый объект без использования отмычек.

Проникнуть на фирму, пускай у двери стоит хоть десяток охранников, зачастую проще простого. Предъявляем паспорт, говорим: кто мы такие и к кому идем. Причем, названное имя не обязательно должно совпадать с именем в паспорте. Объясняем: тот, к кому мы идем, знает нас под сетевым псевдонимом. Охранник звонит указанному лицу и сообщает, что его хочет видеть такая-то личность. Получив "добро" (а "добро" очень часто дается без уточнения подробностей), охранник дает мошеннику "зеленый свет". Разумеется, злоумышленнику вовсе не обязательно

быть сетевым другом одного из сотрудников. Достаточно лишь знать имена его знакомых, выяснить которые не составит никакого труда. (Особенно, если сотрудник злоупотребляет ICQ или Интернет — форумками).

На первый взгляд, знание паспортных данных позволяет без труда найти злоумышленника. Это так, но не стоит обольщаться — доказать его причастность к грамотно спланированной атаке будет очень непросто! Ведь не компьютер же будет выносить в кармане злоумышленник! Вероятнее всего, он постарается подсмотреть набираемый пароль или, обнаружив в пустующем кабинете включенный компьютер, занесет туда шпиона.

Для предотвращения подобных инцидентов следует сопровождать всех посторонних лиц от самого входа до места назначения, не позволяя им самостоятельно бродить по помещению.

СПАМ и все что с ним связано

Массовая рассылка — идеальное средство для поиска простаков. А чужая глупость — отличное средство наживы. В последнее время в сети стало появляться все больше и больше предложений о вложении своих денег в акции. Поразительно, но урок, преподнесенный МММ, так ничему и не научил. Многие по-прежнему обращают внимание лишь на рост котировок, совершенно не интересуясь источником прибыли. А источник-то прост! Фирма, выкинув на биржу акции, через некоторое время сама же скупает их по завышенной цене, чем и привлекает к себе клиентов. Вложения же клиентов идут на очередную закупку акций... Так происходит до тех пор, пока приток клиентов не начинает мельчать, после чего фирма ликвидируется и все акционеры остаются с носом.

Про всевозможные финансовые пирамиды и предложения о заработке огромных куч денег в кратчайшие сроки не стоит и говорить. Если вовремя продав акции, вы еще можете хоть что-то заполучить, то "сетевой заработок" просто откровенная дуриловка, не приносящаяся никакого дохода вообще. Поскольку, это печальное обстоятельство наконец-то стало доходить до любителей халявы, интерес к супер-бизнесу начал мало-помалу ослабевать. Не нужно быть ясновидцем, чтобы предсказать скорого появления сообщений, предлагающих *небольшой* заработок. На фоне остальных это будет выглядеть весьма убедительно, но, тем не менее, останется той же самой ложью.

Кстати, *ни в коем случае не клюйте на объявления о продаже дорогих вещей, пускай по сильно заниженной цене*, т.к. этот трюк широко используется мошенниками для поиска богатых людей со всеми вытекающими отсюда последствиями (в лучшем случае просто ограбят, а в худшем же...).

Вообще, *лучше игнорируйте массовую рассылку, и не отвечайте ни на какие спамерские сообщения*. По-настоящему хорошие товары и способы заработка никогда не рекламируются таким дешевым способом.

Шантаж

Если попытки получить требуемое путем обмана ни к чему не приведут, то злоумышленник может отважиться на прямой шантаж сотрудников фирмы. Статистика показывает, что угроза физической расправы встречается довольно редко, а если и встречается, то в подавляющем большинстве случаев лишь угрозой и остается.

На первом месте лидируют обещания рассказать ревнивому мужу (жене) о супружеской измене — не важно имела ли она место в действительности или нет. Для этого вовсе не обязательно устанавливать скрытые камеры или заниматься фотомонтажом — достаточно быть хорошим рассказчиком, умеющим убедить собеседника. Опасаясь за распад семьи, многие из нас идут на мелкие (с нашей точки зрения) должностные преступления, оборачивающиеся, тем не менее, значительными убытками для фирмы.

Второе место занимают угрозы убедить сына (дочь) в том, что вы не настоящие родители. Поскольку в подростковом возрасте между детьми и родителями часто случаются серьезные конфликты, вероятность того, что ребенок поверит постороннему дяде, чем и нанесет себе тяжелую душевную травму, отнюдь не нулевая!

Способ борьбы с такими шантажистами только один — *полное взаимное доверие между членами семьи*. Руководители фирм должны осознавать, что семейное благополучие сотрудников — залог их, руководителей, безопасности.

В любом случае *никогда не идите на поводу у шантажиста*. Этим вы лишь глубже затягиваете себя в его сети. Напротив, проявив безразличие, вы обезоруживаете мошенника, обесмысливая тем самым шантаж и заставляя его искать другие пути.

Кстати, достаточно широко распространенный способ имитации шантажа для проверки моральной устойчивости сотрудников юридически незаконен. И "подопытный" сотрудник имеет полные основания для подачи иска за нанесенный ему моральный ущерб.

Игра на чувствах

Поскольку шантаж — дело наказуемое, злоумышленники по возможности используют более законные пути. Например, покорив сердце некоторой сотрудницы, мошенник в один прекрасный день может заявить, что он-де проигрался в карты и теперь вынужден долгие годы отрабатывать долг батраком в Казахстане. Правда, есть один вариант... если его пассия скопирует такие-то конфиденциальные документы, он сумеет их продать, тогда никуда уезжать не потребуется и любовный роман продолжится... Впрочем, не обязательно играть именно на любви. Ничуть не хуже толкает на преступление алчность, желание отомстить руководству или попытка самоутвердиться.

Множество подобных авантюр совершаются по ICQ, что чрезвычайно осложняет поиски злоумышленника. Поэтому, администраторам настоятельно рекомендуется запретить пользоваться ICQ всему персоналу или, на худой конец, хотя бы

контролировать содержимое разговоров. (Безнравственно, конечно, но что поделаешь). Разумеется не стоит забывать и об электронной почте. А еще лучше *не принимать на ответственные должности романтических или психологически неуравновешенных лиц*, даже если они хорошие специалисты.

Заключение

Разговор о секретах социальной инженерии можно продолжать бесконечно, но это все равно не защитит вас от злоумышленников и мошенников всех мастей. Среди них нередко попадаются весьма талантливые люди, проворачивающие на редкость изощренные комбинации, перед которым снял бы шляпу и сам Остап Бендер. Поэтому типовых противодействий социальным инженерам не существует и не может существовать! Каждая ситуация требует индивидуального подхода и всестороннего рассмотрения.

Единственная рекомендация — не допускайте бардака ни у себя дома, ни на работе. Расхлябанность, отсутствие дисциплины, халатность — вот главные дыры в системе безопасности, не компенсируемые ни какими, даже 1024-битными системами шифрования. Помните, что *скупой платит дважды*. Экономия на собственной безопасности до добра еще никого не доводила.