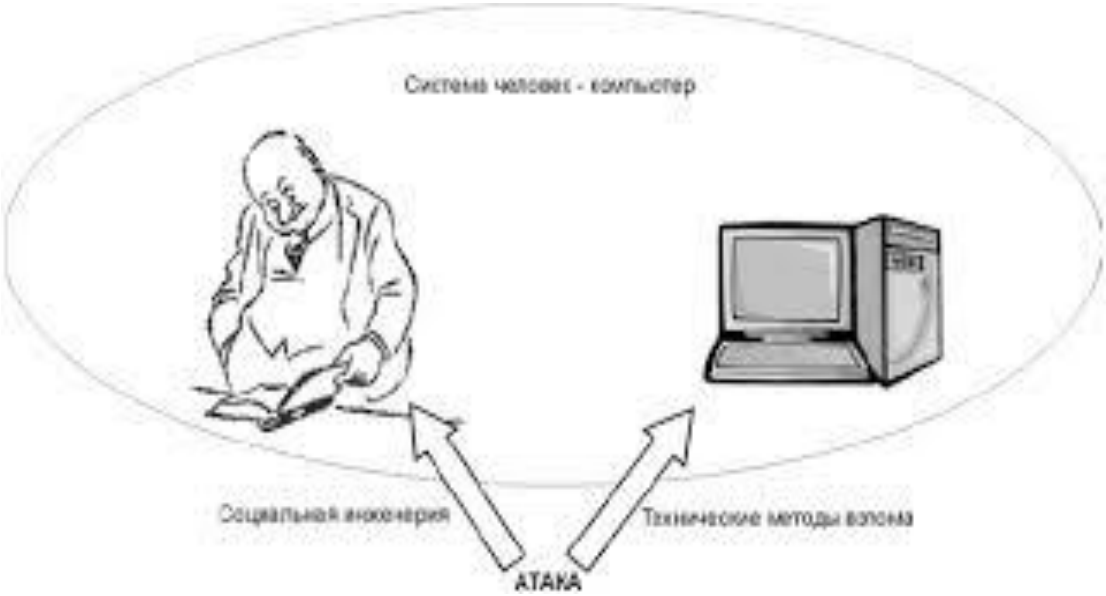
Социальная инженерия

Социальная инженерия - это метод манипуляции действиями человека, заключающийся в использовании слабостей человеческого фактора в целях незаконного получения личной информации (учетных или банковских данных) или несанкционированного доступа к компьютеру жертвы с целью установки на него вредоносного ПО. **Социальная инженерия** – метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Основной целью социальной инженерии является получение доступа к конфиденциальной информации, паролям, банковским данным и другим защищенным системам.

- Самое слабое звено защиты любой системы - сами пользователи. Социальная инженерия пытается использовать присущие людям слабости
- в целях получения конфиденциальной информации и последующего доступа в систему.

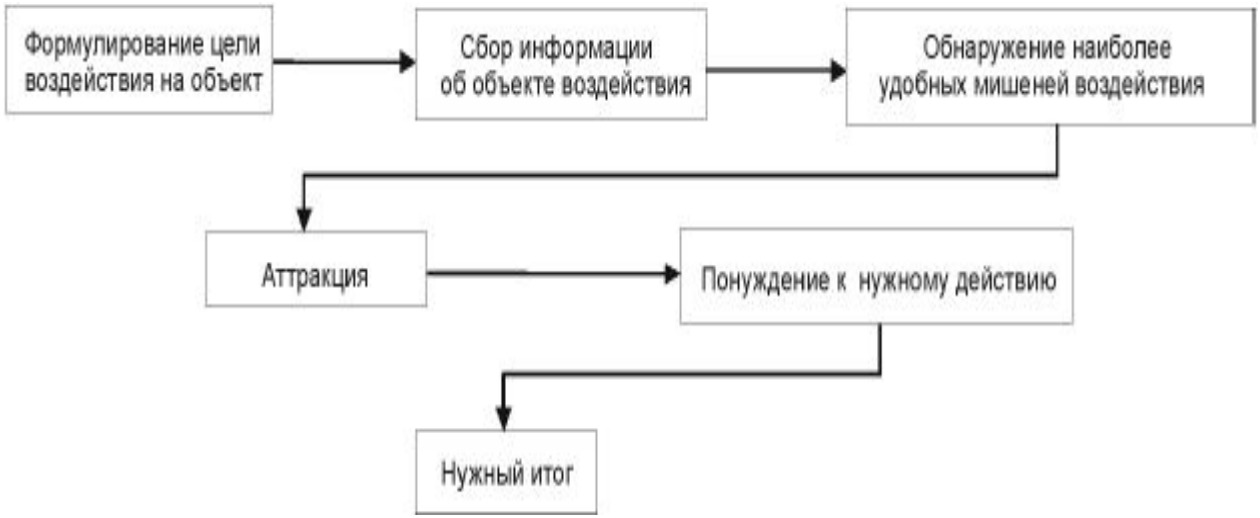

Система человек - компьютер
Социальная инженерия
Технические методы взлома
АТАКА

- Мошенники часто прибегают к подобной практике, так как с помощью нее значительно проще добыть учетные данные, нежели получить их путем взлома системы безопасности.
- Основным отличием социальной инженерии является стремление злоумышленников с её помощью обойти все технические средства защиты, избрав основным вектором атаки человека, а не систему вашего компьютера.


Финансовые махинации
Проникновение в структуру организации для дестабилизации основных узлов сети
Общая дестабилизация работы организации с целью снижения ее влияния и последующего полного разрушения
Доступ к персональным данным
ОБЛАСТИ ПРИЛОЖЕНИЯ ДЕСТРУКТИВНЫХ ВОЗДЕЙСТВИЙ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ
Хищение конфиденциальных сведений
Ведение конкурентной разведки
Получение информации о маркетинговых и др. планах организации
Получение конфиденциальной информации
Получение информации о перспективных сотрудниках для их вывода из организации

Техники и методы внедрения

Обобщенная схема атаки при помощи социальной инженерии



- **Источники социальной инженерии**
- Среди наиболее популярных методов социальной инженерии можно выделить следующие: Бейтинг или лов "на живца" (пользователь обманным путем заманивается на сайт злоумышленников, после чего на его компьютер устанавливается вредоносное ПО), фишинг (отправка мошеннических сообщений с целью получения конфиденциальных данных), вишинг (использование системы предварительно записанных голосовых сообщений для выманивания личных данных) или лже-антивирус (использование ложных сообщений о заражении системы ПК и его лечении программным обеспечением, которое заражает компьютер).

Необходимо остерегаться любых незапрошенных предложений помощи, в особенности предлагающих переход по сторонним ссылкам. Как правило, в подобных случаях речь идет об уловках социальной инженерии. Данное правило тем более актуально, если от пользователя требуется указать учетные или банковские данные. В таком случае без всяких сомнений речь идет о мошенничестве, так как уважающие себя финансовые организации ни при каких обстоятельствах не будут запрашивать учетные данные посредством сообщения эл. почты. Кроме того, настоятельно рекомендуем проверить адрес отправителя кажущегося вам подозрительным сообщения эл. почты и убедиться в его легитимности.

Социальная инженерия нематериальна, ее невозможно физически устранить. Самый эффективный способ не стать жертвой социальной инженерии - не терять бдительности и не позволять злоумышленникам себя провести. Ввиду того, что методы социальной инженерии разработаны профессионалами своего дела, распознать обман порой не под силу даже специалистам. Именно поэтому наиболее эффективным способом защиты по-прежнему является использование современного антивирусного решения, которое распознает и отстранит все типы вредоносного ПО, а также надежного менеджера паролей, который поможет создать невзламываемые пароли и хранить их в безопасности.


ОБМАН СОТРУДНИКА (системного администратора, секретаря в приемной, оператора call-центра, менеджера по работе с клиентами, охранника на посту, адресата почты или телефонного вызова)
ПРОНИКНОВЕНИЕ НА ТЕРРИТОРИЮ
QUID PRO QUO
IVR (телефонный фишинг)
ФИШИНГ
PRETEXTING
ВЫЯСНЕНИЕ И ПОЛУЧЕНИЕ ТЕЛЕФОННЫХ НОМЕРОВ, ПАРОЛЕЙ, СВЕДЕНИЙ
ПЛЕЧЕВОЙ СЕРФИНГ
ПРЯМАЯ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ
ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ОТКРЫТЫХ КАНАЛОВ ТЕЛЕКОММУНИКАЦИЙ (телефон, электронная почта, фальшивые интернет-сайты, служба мгновенного обмена СМС, социальные сети)
ОБРАТНАЯ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ
ИЗУЧЕНИЕ И АНАЛИЗ ИНФОРМАЦИОННОЙ СФЕРЫ ОБЪЕКТА
НЕСАНКЦИОНИРОВАННАЯ СМЕНА ПАРОЛЕЙ
ОРГАНИЗАЦИЯ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ЗАКРЫТЫМ КАНАЛАМ ПЕРЕДАЧИ И БАЗАМ ДАННЫХ
ПОДБРОС ИНФИЦИРОВАННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ («ДОРОЖНОЕ ЯБЛОКО»)
СОЗДАНИЕ УЧЕТНЫХ ЗАПИСЕЙ (С ПРАВАМИ ПОЛЬЗОВАТЕЛЯ ИЛИ АДМИНИСТРАТОРА)
ВНЕДРЕНИЕ ТРОЯНСКИХ ПРОГРАММ
ТЕХНОЛОГИЧЕСКОЕ ВСКРЫТИЕ И ПРИМЕНЕНИЕ СПОСОБОВ УДАЛЕННОГО ДОСТУПА
НЕСАНКЦИОНИРОВАННОЕ ДОБАВЛЕНИЕ ДОПОЛНИТЕЛЬНЫХ ПРАВ И ВОЗМОЖНОСТЕЙ ЗАРЕГИСТРИРОВАННЫМ ПОЛЬЗОВАТЕЛЯМ СИСТЕМЫ

Претекстинг

- это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую-либо информацию или совершить определенное действие. Чаще всего данный вид атаки предполагает использование голосовых средств, таких как Skype, телефон и т.п.
- Для использования этой техники злоумышленнику необходимо изначально иметь некоторые данные о жертве (имя сотрудника; должность; название проектов, с которыми он работает; дату рождения). Злоумышленник изначально использует реальные запросы с именем сотрудников компании и, после того как войдет в доверие, получает необходимую ему информацию.

Фишинг

- техника интернет-мошенничества, направленная на получение конфиденциальной информации пользователей - авторизационных данных различных систем. Основным видом фишинговых атак является поддельное письмо, отправленное жертве по электронной почте, которое выглядит как официальное письмо от платежной системы или банка. В письме содержится форма для ввода персональных данных (пин-кодов, логина и пароля и т.п) или ссылка на web-страницу, где располагается такая форма. Причины доверия жертвы подобным страницам могут быть разные: блокировка аккаунта, поломка в системе, утеря данных и прочее.

Троянский конь

- это техника основывается на любопытстве, страхе или других эмоциях пользователей. Злоумышленник отправляет письмо жертве посредством электронной почты, во вложении которого находится «обновление» антивируса, ключ к денежному выигрышу или компромат на сотрудника. На самом же деле во вложении находится вредоносная программа, которая после того, как пользователь запустит ее на своем компьютере, будет использоваться для сбора или изменение информации злоумышленником.

Кви про кво (услуга за услугу)

- данная техника предполагает обращение злоумышленника к пользователю по электронной почте или корпоративному телефону. Злоумышленник может представиться, например, сотрудником технической поддержки и информировать о возникновении технических проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе «решения» такой проблемы, злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое программное обеспечение на компьютере жертвы.

Дорожное яблоко

- этот метод представляет собой адаптацию троянского коня и состоит в использовании физических носителей (CD, флэш-накопителей). Злоумышленник обычно подбрасывает такой носитель в общедоступных местах на территории компании (парковки, столовые, рабочие места сотрудников, туалеты). Для того, чтобы у сотрудника возник интерес к данному носителю, злоумышленник может нанести на носитель логотип компании и какую-нибудь подпись. Например, «данные о продажах», «зарплата сотрудников», «отчет в налоговую» и другое.

Обратная социальная инженерия

- данный вид атаки направлен на создание такой ситуации, при которой жертва вынуждена будет сама обратится к злоумышленнику за «помощью». Например, злоумышленник может выслать письмо с телефонами и контактами «службы поддержки» и через некоторое время создать обратимые неполадки в компьютере жертвы. Пользователь в таком случае позвонит или свяжется по электронной почте с злоумышленником сам, и в процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные.

Методы защиты

Для защиты от техник социальной инженерии следует соблюдать некоторые правила:

- не использовать один и тот же пароль для доступа к внешним и корпоративным ресурсам;
- не открывать письма, полученные из ненадежных источников;
- блокировать компьютер, когда не находитесь на рабочем месте;
- установить антивирус;
- ознакомиться с политикой конфиденциальности компании. Все сотрудники должны быть проинструктированы о том, как вести себя с посетителями и что делать при обнаружении незаконного проникновения;
- обсуждать по телефону и в личном разговоре только необходимую информацию;
- необходимо удалять все конфиденциальные документы с портативных устройств.

Угрозы безопасности, связанные с электронной почтой и с использованием службы мгновенного обмена сообщениями

Законодательсво РФ

"Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 26.08.2017)

УК РФ Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяниеовлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, - наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, - наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

(в ред. Федерального закона от 28.06.2014 N 195-ФЗ)

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, - наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.

Примечания:

- Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.
- Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

1. Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, -

   наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, -

   наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, - наказываются лишением свободы на срок до семи лет.

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, - наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.
2. Деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления, - наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, - наказываются принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации, - наказывается принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до шести лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, - наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

4. Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения, - наказываются лишением свободы на срок от трех до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

5. Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они повлекли тяжкие последствия, - наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.