Информзащита

Криминологическая характеристика преступлений против собственности, совершаемых с использованием ИКТ

1. Понятие социальной инженерии

Социальная инженерия –

- **социальная инженерия** — это один из разделов социальной психологии, направленный на то, чтобы внедрять в их сознание некоторую модель поведения и тем самым манипулировать их поступками.

- **социальная инженерия** — это метод (атак) несанкционированного доступа к информации или системам хранения информации без использования технических средств. Метод основан на использовании слабостей человеческого актора и считается очень разрушительным.

- **социальная инженерия** — это набор прикладных психологических и аналитических приемов, которые злоумышленники применяют для скрытой мотивации пользователей публичной или корпоративной сети к нарушениям устоявшихся правил и политик в области информационной безопасности.

Информзащита
Учебный центр

В общем виде схема воздействия имеет вид, показанный на рисунке

Сканирование (Обнаружение потенциальной уязвимости) → **Выявление «точки входа»** (Эмоционально-рациональный анализ объекта) → **Аттракция** (Создание сценариев – нужных условий для влияния)

2. Преступные техники социальной инженерии

Вид техники:

Фишинг (англ. *fishing* — рыбалка)

- **Жертва получает фальсифицированное письмо, содержащее ссылку на какой-либо сайт, не вызывающий явных подозрений. Перейдя по ней, пользователь, сам того не понимая, выкладывает свои логины и пароли злоумышленникам. Также нередки случаи, когда данные похищаются с помощью QR-кодов и других «прямых» ссылок. Техника фишинга основана на том, что человек склонен верить в надежность именитых брендов, связывая их с авторитетностью**

Типы фишинговых атак:

1) с помощью **мошенничества**, когда пользователь обманывается мошенническими электронными письмами с целью раскрытия личной или конфиденциальной информации

Вт 06.12.2016 18:05

info@vtb24.ru

Уведомление о задолженности

Кому [redacted]

ВТБ24

Большое преимущество

Здравствуйте, Павел [redacted]!

Кредитный отдел ВТБ 24 (ПАО), Уведомляет Вас о том, что на Ваше имя 20.09.2015 был оформлен потребительский кредит через наш онлайн банкинг на сумму

680 000 рублей.

На данный момент задолженность не погашена. На 01.12.2016 Ваш долг составляет

663 773 рублей с учетом пени (0.7% в сутки).

В связи с этим на Ваше имя ВТБ 24 (ПАО) был составлен судебный иск.

Ознакомится с документами Вы можете по ссылке в личном кабинете

В случае Вашей неявки на заседание суда мы будем вынуждены поставить Вашего работодателя в известность о вышеуказанных фактах.

С уважением,
ВТБ 24 (ПАО)

Типы фишинговых атак:

2) с помощью **вирусного программного обеспечения**, когда злоумышленнику удается запустить опасное программное обеспечение на компьютере пользователя

вредоносное программное обеспечение, записывающее каждое нажатие клавиши на вашем компьютере

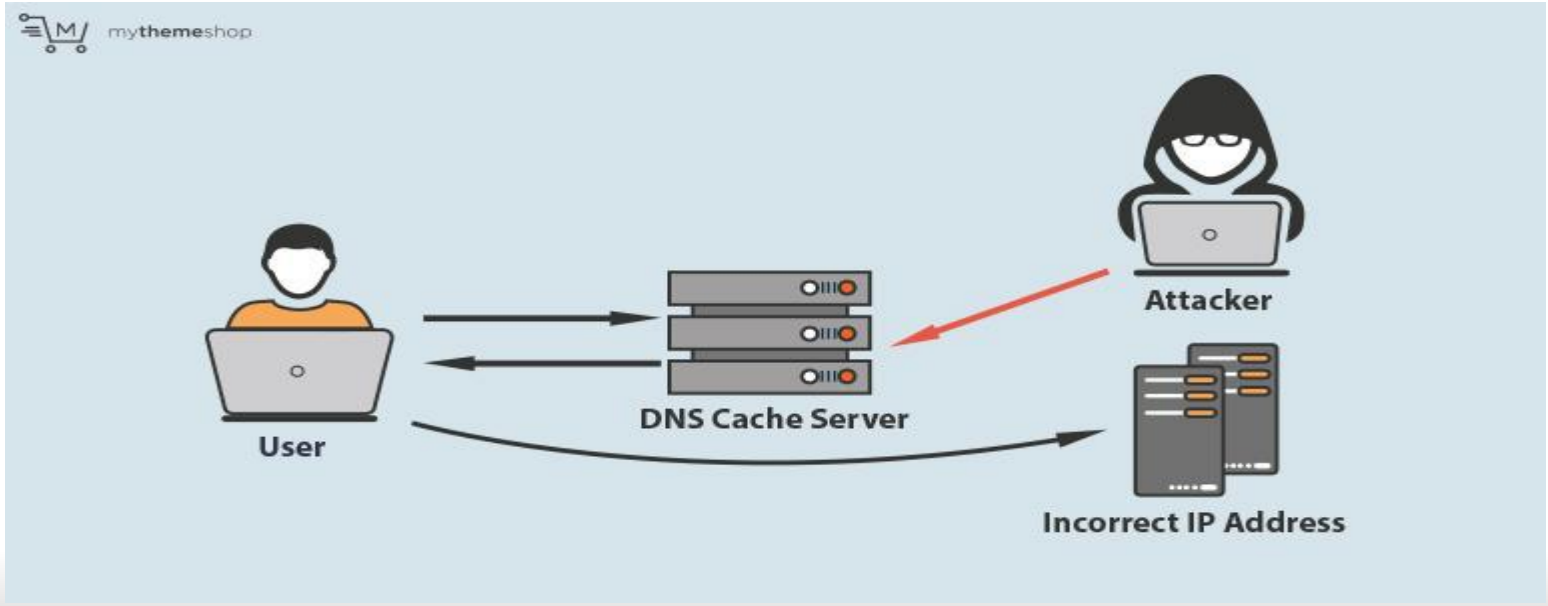
Типы фишинговых атак:

3) с использованием **DNS-спуфинга**, когда злоумышленник компрометирует процесс поиска домена, для того чтобы пользователь выбрал вместо настоящего веб-сайта – поддельный

Типы фишинговых атак:

DNS-атака

IP-адрес веб-сайта на ворованный IP-адрес, то любой челЕсли в любой учетной записи хакер сможет найти способ заменить разрешенный овек, пытающийся получить доступ к этому веб-сайту, будет отправлен на поддельный адрес. Пользователь не будет иметь и малейшего понятия, что он обращается к неправильному адресу.



Информзащита
Учебный центр

Типы фишинговых атак:

4) путем **вставки вредоносного контента**, когда злоумышленник помещает вредоносный контент в обычный веб-сайт

Коллекция | Ш | Стар

Обнаружено вредон

php.net

Google | Новая вкладка | forum.opennet.ru | Другие закладки

chrome

Веб-сайт, на который вы хотите перейти, содержит вредоносное ПО!

Google Chrome заблокировал доступ к php.net.

Даже если в прошлом вы посещали этот веб-сайт без последствий, в этот раз ваш компьютер может заразиться вредоносным ПО.

Вредоносное ПО – это программное обеспечение, специально созданное для совершения преступных действий, например хищения идентификационных данных, кражи денег или безвозвратного удаления файлов. Подробнее...

Назад

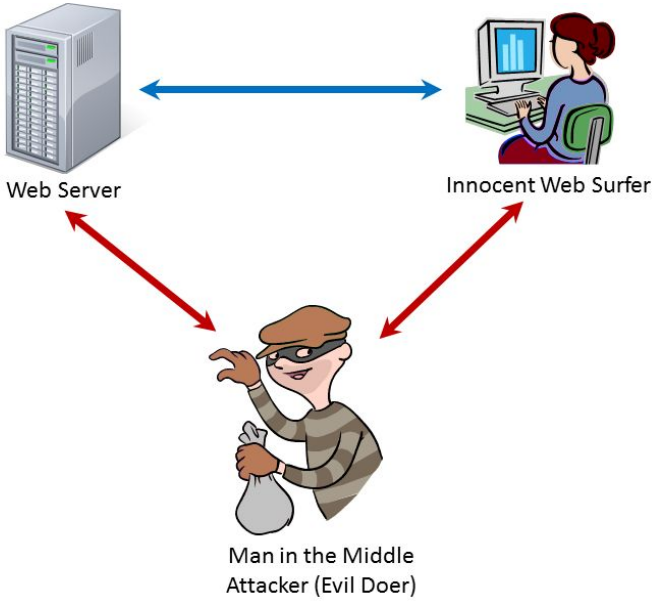
Подробнее о проблемах

Продолжить на свой страх и риск «

Типы фишинговых атак:

5) с использованием подхода MITM (Man in the middle – атака посредника, или атака «человек посередине») – вид атаки в криптографии, когда злоумышленник встает между пользователем и компрометируемым сайтом и вносит изменения в соединение, либо осуществляет хищения информации пользователя

Типы фишинговых атак:



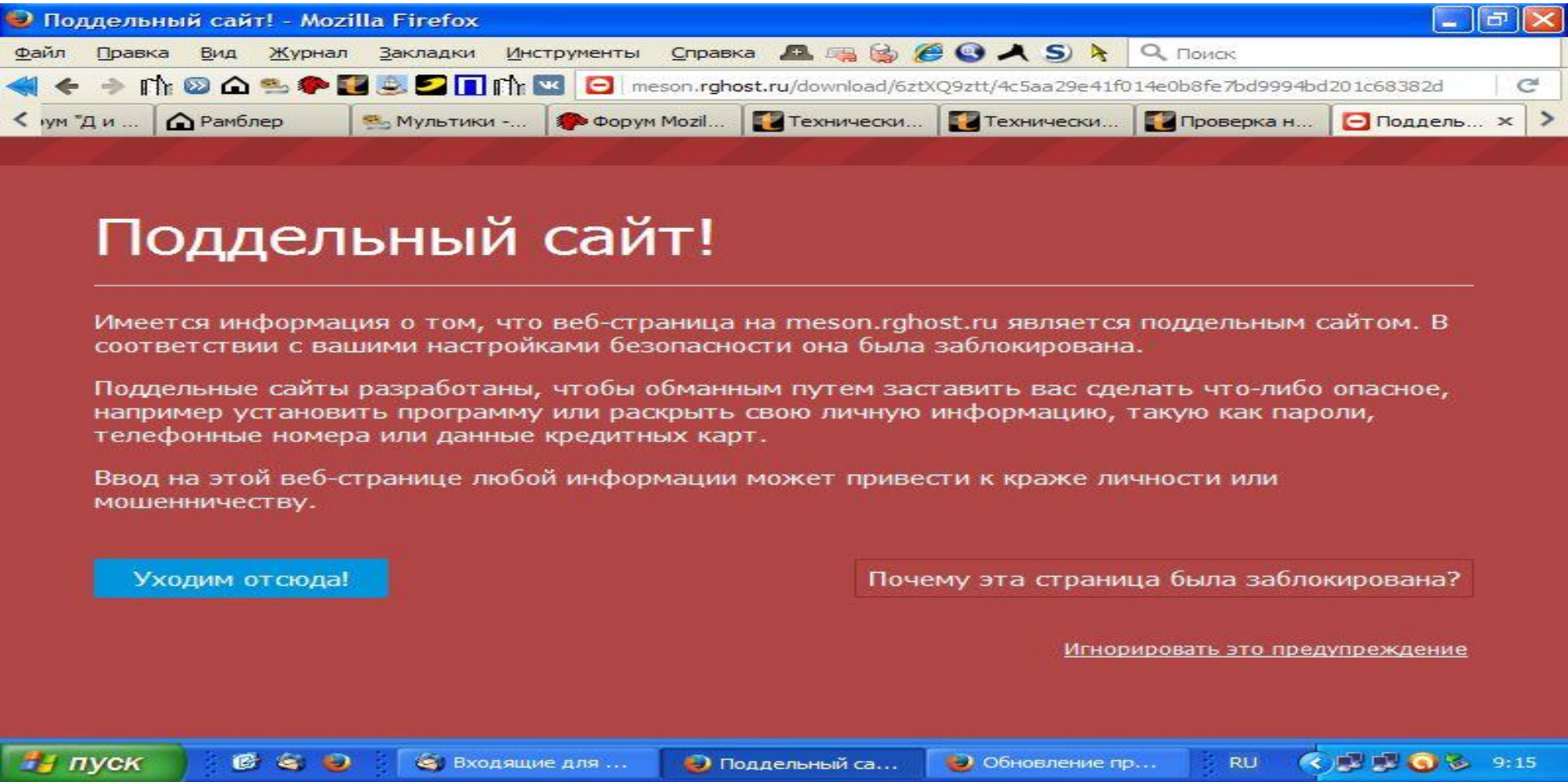
Злоумышленнику надо всего лишь поставить себя в цепь между двумя общающимися сторонами, чтобы перехватывать их сообщения друг другу. При этом злоумышленник всегда должен выдавать себя за каждую из противоположных сторон

Типы фишинговых атак:

7) с помощью индексации поисковой системой, где поддельные вебстраницы с привлекательными предложениями, созданными злоумышленником, индексируются поисковой системой, чтобы пользователь мог наткнуться на нее

Типы фишинговых атак:

Индексация сайта значит, что робот поисковой системы посещает ресурс и его **страницы**, изучает контент и заносит его в базу данных. Впоследствии эта информация выдается по ключевым запросам



Вид техники:

Претекстинг

(англ. *Pretexting* — заранее составленный сценарий)

- **Осуществляется с помощью онлайн-мессенджеров или просто по телефону. Данный метод требует от синжера предварительной подготовки — сбора информации, как правило, из открытых источников (социальные сети, базы данных операторов связи и т. п), для обеспечения определенного уровня доверия цели.**

В результате жертва, проникнувшись к злоумышленнику, сообщает конфиденциальную информацию и/или совершает определенное действие, несущее угрозу безопасности компании.

Вид техники:

Кви про кво
(лат. *Quid pro quo* — то за это)

- **Чаще всего злоумышленник звонит в компанию, представляясь сотрудником технической поддержки. В процессе разговора он узнает о наличии каких-либо проблем. В случае если они есть, мошенник по телефону по¬могает сотруднику компании «решить» их, в процессе чего последний собствен¬норучно вводит команды, запускающие вредоносное программное обеспечение.**

Вид техники:

Троянская программа

- Тип программного обеспечения создан для несанкционированного удаленного проникновения на компьютер пользователя. Злоумышленник отправляет электронное письмо, содержащее, например, муляж важного обновления антивируса, представленного в виде ссылки, после перехода по которой в устройство проникает троян. В отличие от обычного вируса, он не имеет функции размножения и дальнейшего распространения по сети. Однако троян открывает дверь для проникновения других вирусов.

Вид техники:

Дорожное яблоко

- Это методика, в основе которой лежат те же принципы, что и у «Троянского коня». Разница лишь в использовании зараженных физических носителей (flash-диски, CD-диски и т. д.), подделываемых под официальные и подбрасываемых работнику компании. Статистика показывает, что данный метод является самым успешным, когда речь идет об атаке на крупную компанию

Вид техники:

Обратная социальная инженерия

- Вид атаки, при которой злоумышленником создается такой сценарий, в котором жертва сама будет вынуждена обратиться к нему за помощью. Например, никто в здравом уме не сообщит пароль от социальной сети незнакомому человеку. Однако звонок в 8 утра в воскресенье от «сотрудника технической поддержки» по поводу устранения важных неполадок может развязать пользователю язык

Откуда берутся профессионалы – синжеры?

- **Социальный инжиниринг образовался как отдельная часть из прикладной психологии**.
- Ему обучают шпионов, агентов влияния, завербованных неформальных лидеров. Все техники социального инжиниринга основаны на особенностях принятия решений людьми, называемых когнитивным базисом.
- Умение расположить к себе ранее не знакомого собеседника по телефону, в целях получения необходимой информации или просто заставить его что-то сделать, приравнивается к искусству манипулирования.
- Профессионалы по наводящим вопросам, интонации голоса, могут определить комплексы и страхи человека и сориентировавшись мгновенно использовать их.

Роль синжера:

1. Хакеры

- Как известно, «любая система небезопасна, пока в ней присутствует человек». Хакеры, охотясь за какой-либо информацией, зачастую применяют техники социального взлома, ведь современные информационные сети надежно защищены от угроз извне, в отличие от рядовых сотрудников

Роль синжера:

2. Воры личной информации

- Данный вид социальных инженеров использует такую информацию, как, например, имя человека, номер банковского счета или дату рождения без ведома владельца. Чаще всего эти данные собираются для гораздо большего преступления.

Роль синжера:

3. Коммерческие социальные инженеры

- В данный класс входят люди, которые с помощью социальной инженерии выуживают деньги из людей, в основном по телефону и в Интернете

Роль синжера:

4. Пентестеры

- Это люди, которые в учебных целях проводят санкционированные атаки на информационную систему компании для выявления потенциальных уязвимостей. Они не используют полученную информацию для личной выгоды, а лишь указывают на ошибки в системе безопасности

3. Причины и условия телекоммуникационных преступлений

Условия и факторы возникновения телекоммуникационных преступлений.

- Предоставление операторами связи контента телекоммуникационных услуг не прошедших проверку на уязвимость.
- Отсутствие следственной и судебной практики по сложным составам телекоммуникационных преступлений.
- Человеческий фактор – основная причина незащищенности от преступных посягательств.
- Слабая законодательная база, отсутствие сертифицированных специалистов, привлекаемых судами в качестве экспертов при расследовании сложных телекоммуникационных преступлений.
- Существующий порядок заведения дел оперативного учета включает в себя ряд ограничений, сдерживающих оперативность при проведении проверочных мероприятий.
- Большинство телекоммуникационных преступлений обладают латентной формой протекания, что усложняет своевременность их выявления.
- Существующие меры уголовной ответственности не являются сдерживающим фактором для злоумышленников.
- Следственные органы, на территории которого реализуется ДОУ, как правило, не заинтересованы в расследовании тех эпизодов преступления, которые совершены за пределами их юрисдикции.
- Отсутствует регламент взаимодействия между государственными надзорными службами по работе с интернет провайдерами, операторами связи и федеральными надзорными органами.

Существующие меры ответственности в России не являются сдерживающим фактором для преступников.

Как у нас

- **Статья 159.6. Мошенничество в сфере компьютерной информации**
- [Уголовный кодекс РФ] [Глава 21] [Статья 159.6]
- **Ч.1.** Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, -
- наказывается штрафом в размере до ста двадцати тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо обязательными работами на срок до трехсот шестидесяти часов, 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 арестом на срок до четырех месяцев.

Как у них

- В начале мая 2015 года на рассмотрение Конгресса США был представлен законопроект Cyber Security Enhancement Act, ужесточающий ответственность за преступления в сфере компьютерных технологий. Кроме того, впервые планируется введение наказания за совершение преступлений с использованием бот-сетей.

http://www.delfi.lv/tech/tehnologii/vlasti-ssha-uzhestochat-otvetstvennost-za-kiberprestupleniya.d?id=17906971#ixzz3aaOnadZr

- **В 1979 г. на Конференции Американской ассоциации адвокатов** в г. Далласе впервые в США была сформулирована система компьютерных преступлений, ставшая затем основой для уголовного законодательства штатов. Закон установил уголовную ответственность за сам факт неразрешенного доступа к чужой компьютерной информации. Он стал основным нормативным правовым актом, устанавливающим уголовную ответственность за преступления в сфере компьютерной информации, включенный в виде § 1030 в Титул 18 Свода законов США.

Существующие меры ответственности в России не являются сдерживающим фактором для преступников.

Как у нас

- **Статья 159.6. Мошенничество в сфере компьютерной информации**
- [Уголовный кодекс РФ] [Глава 21] [Статья 159.6]
- 3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные лицом с использованием своего служебного положения, а равно в крупном размере, -
- наказываются штрафом в размере от ста тысяч до пятисот тысяч рублей…, либо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев либо без такового и с ограничением свободы на срок до полутора лет либо без такового.
- 4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, наказываются лишением свободы на срок до десяти лет со штрафом в размере до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период до трех лет либо без такового и с ограничением свободы на срок до двух лет либо без такового.

Как у них

- В случае, если злоумышленник проникает в компьютерные сети инфраструктуры США - телевизионные сети, энергосети, транспортные каналы связи, системы управления водоснабжением, газификации, защищенные абонентские компьютеры - то уголовное наказание по таким видам преступлений всегда максимальное и осужденный может быть приговорен к 30 годам заключения без права досрочного освобождения.
- Один из разделов закона посвящен компьютерному шпионажу и предусматривает уголовное наказание за хищение интеллектуальной собственности американских компаний. В разделе обговариваются и сроки заключения для приговоренных судом по этим обвинениям, они увеличиваются с 15 до 20 лет.

4. Противодействие методам социальной инженерии

Без борьбы с мошенничеством на финансовом рынке страна не сможет нормально развиваться.

- Законодатели понимают, что современные кредитно-финансовые инструменты при всей своей пользе и привлекательности имеют серьёзные операционно-технические уязвимости.
- В Государственной думе РФ готовят законопроект об усилении ответственности за хищение электронных денежных средств.
- Президент Владимир Путин предложил дать Следственному комитету РФ дополнительные полномочия. Речь идет о следующих экспертизах: молекулярно-генетическая…. финансово-аналитическая и другие.

Информзащита
Учебный центр

Выделяют три вида средств противодействия методам социальной инженерии

- Административный
- Антропогенный
- Технический

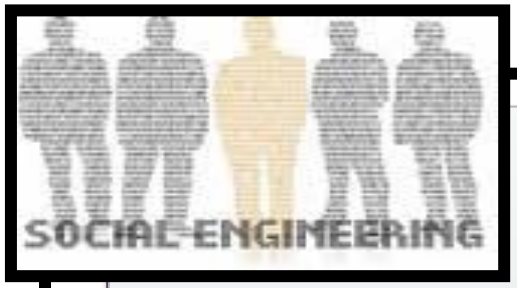
Информзащита
Учебный центр

1. Административный

Все работники компании независимо от занимаемой должности обязаны понимать ценность информации, с которой им приходится работать

1. Административный

Градация осознания ценности информации^



Служебная тайна

Конфиденциальная информация

Ценность информации осознается руководством, но не осознается персоналом

Информация, ценность которой не осознается её собственником.

Информзащита
Учебный центр

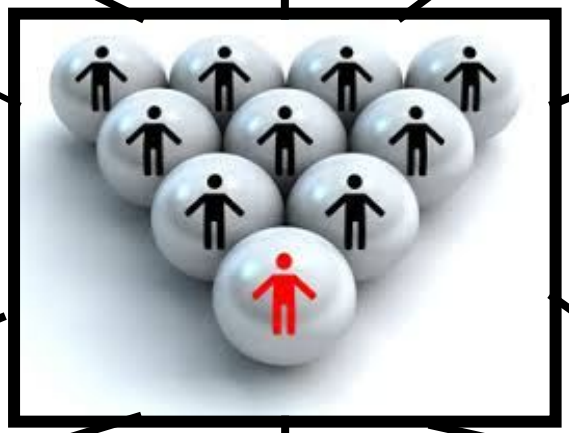
2. Антропогенный

— привлечение внимания людей к вопросам безопасности с помощью объявлений, баннеров социальной рекламы и т. п.;

— осознание пользователями всей серьезности проблемы и принятие политики безопасности системы;

— изучение и внедрение необходимых методов и действий для повышения защиты информационного обеспечения.

Внедрение политик противодействия социальной инженерии в коллективе.



- Инструктажи
- Рассылка информационных статей
- «Самый надежный сотрудник месяца»
- Коллективный разбор инцидентов
- Плакаты в помещениях
- «Провокации» службы безопасности
- Раздача печатных вкладышей
- Наклейки на стационарных телефонах
- Напоминания через голосовую почту
- Экранные заставки на мониторах

Инструктаж сотрудников: все просто, как апельсин.

- не используйте один и тот же пароль для доступа к внешним и корпоративным ресурсам;
- не открывайте письма, полученные из ненадежных источников;
- блокируйте компьютер, когда не находитесь на рабочем месте;
- ознакомьтесь с политикой конфиденциальности вашей компании;
- обсуждайте по телефону и в личном разговоре только необходимую информацию;
- Соблюдение протокола BYOD – не храните любые конфиденциальные документы в памяти личных гаджетов.

3. Технический

1) помешать получить конфиденциальную информацию. К данному способу можно отнести:

— ограничение прав сотрудника в системе — запрет на доступ к «нежелательным» web-сайтам и использование съемных носителей;

— использование системы обнаружения и предотвращения атак в корпоративной сети компании;

— наличие обязательных регламентов безопасности, а также инструкций, находящихся в постоянном доступе сотрудников и содержащих в себе порядок действий при возникновении различных угроз безопасности;

— четкое разграничение информации, получаемой каждым сотрудником, для исключения возможности получения всего пакета сведений при «взломе» одного человека;

3. Технический

2) помешать воспользоваться полученной информацией. К данному способу относятся:

— привязка аутентификационных данных к ip, серийным номерам и электронным подписям;

— авторизация по системе Captcha;

— использование двухфакторной аутентификации.

Заключение.

Синжеры талантливы и изобретательны, поэтому НИКТО и НИКОГДА не может на 100% защитить Вас от информационных атак с применением методов социальной инженерии.

Благодарим за внимание.

Информзащита
Учебный центр