

Социальная инженерия

Или как заставить человека выдать пароль?

Вопросы по предыдущим темам или ДЗ

Mini-quize по прошлым темам:

1. Почему банки атакуют троянами?
2. Почему такое широкое применение получил ассиметричный алгоритм шифрования?
3. В чем отличие симметричного и ассиметричного шифрования?
3. Как зловредный код попадает в приложение?
4. Что такое BotNet?
5. В чем отличие DOS от DDOS

Mini-quize по новой теме:

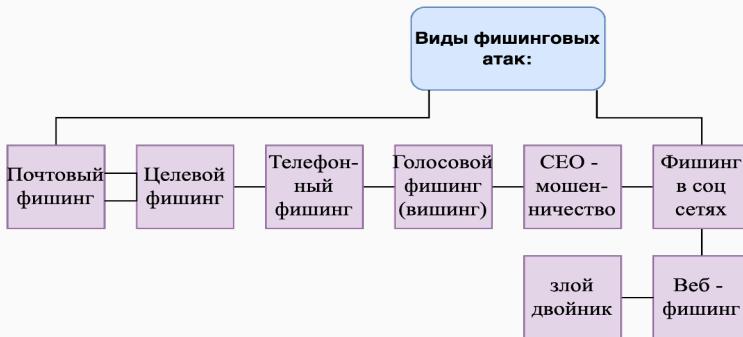
- 1. Что такое фишинг и чем он отличается от спама?**
- 2. Как вы думаете, почему самый уязвимой точкой инфраструктуры считается человек?**

План занятия

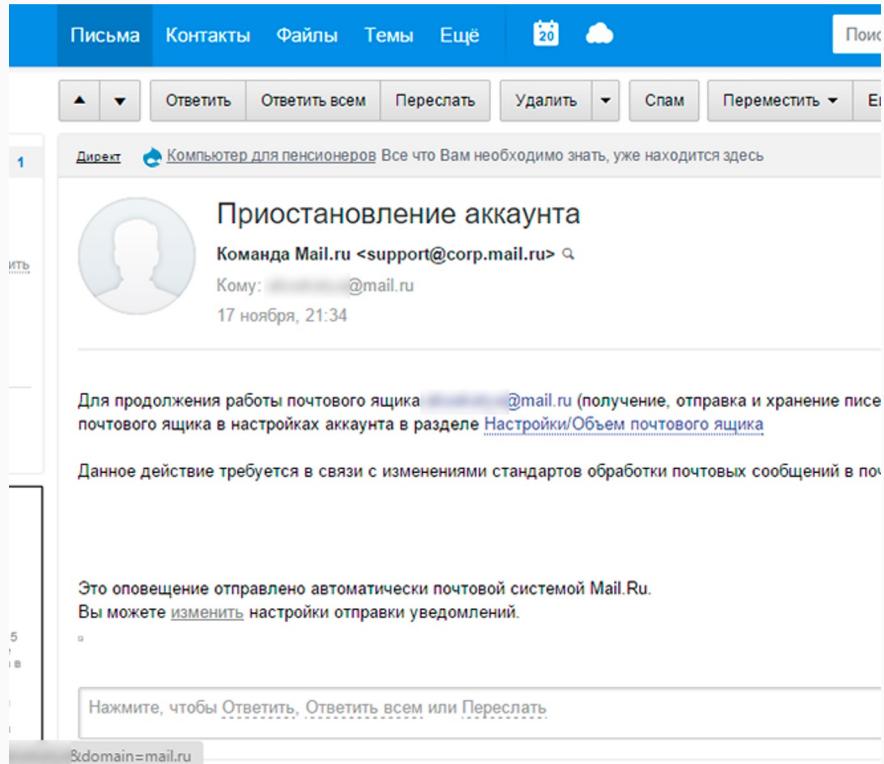
1. Разберем, что такое фишинг, чем он опасен и с чем его едят.
2. Изучим примеры социальной инженерии и проанализируем как можно попасть в компанию.
3. Разберемся, кто такие инсайдеры и почему их так не любят компании.
4. Разберемся почему обратная социальная инженерия страшнее чем прямая.

ФИШИНГ#1

Фишиング – вид мошенничества, направленный на доступ к личным/конфиденциальным данным.



1. Вишинг
2. Смишинг
3. Охота на китов
4. Точечный фишинг



Пример фишингового письма

Фишинг#2 Методы реализации фишинга:

- осуществление массовой рассылки электронных писем от имени знаменитых брендов;
- рассылка личных сообщений от имени Банков;
- получение информации из внутренней переписки внутри социальных сетей;
- использование фиктивных сайтов, похожих на официальный сайт Банка, на которых правонарушители пытаются побудить пользователя ввести свои логин и пароль от электронного банка, а также иную персональную информацию;
- использование поддельных сайтов интернет-магазинов/ туроператоров с крайне «доступными» ценами, за брендовые товары/ путешествия/ авиабилеты. В итоге есть вероятность заплатить за товар/ услугу, которые никогда не будут получены, так как их никогда не существовало.

Фишинг#3 Как защититься?

- Проверять доменное имя сайтов, на которых необходимо ввести персональные данные.
- Не доверять сообщениям, которые просят внести личные данные, лучше созвониться с банком и уточнить информацию (если правонарушители представляются работниками Банка).
- Регулярно обновлять антивирусное ПО. Критически оценивать «выгодные» предложения.

рекомендации

ФИШИНГ#2

Вишиング – это один из методов, который заключается в том, что злоумышленники, используя телефонную связь и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя банковской платежной карточки конфиденциальную информацию или стимулируют к совершению определенных действий с карточным счетом/платежной карточкой с целью хищения денежных средств.



НЕ РАССКАЗЫВАЙ!

- * Пин-код от карты
- * CVV (3-х значный код на оборотной стороне карты)
- * Баланс на карте
- * Логин и пароль от интернет-банкинга
- * Срок действия карты
- * Паспортные данные

ФИШИНГ#3

Скимминг - кража данных карты при помощи специального считывающего устройства



Скиммеры – устройства, для кражи данных.

[Как защититься](#)

Фишинг#4

«Охота на китов» (англ. whaling). Это — атака на топ-менеджмент компании с целью получения доступа к экономической или стратегической информации. Часто нападение производится с помощью сайтов, которые посещают руководители компаний определенного сектора экономики.



Фишинг#5

Кардинг — вид мошенничества, при котором хакеры совершают операцию с использованием платежной карты без участия ее владельца.



[Более подробная информация](#)

Фишинг: главное

- Это вид мошенничества, целью которого является похищение личных данных в интернете.
- Фишинг угрожает не только отдельным людям, но и организациям. Утечка данных клиентов плохо сказывается на репутации компании.
- Самое эффективное оружие в борьбе с фишингом — бдительность. Проверяйте ваши письма и ссылки.
- Установите антивирус, настройте спам-фильтры и двухфакторную аутентификацию, где это возможно.



Social Engineering



В этом углу у нас
брандмауэры,
криптосистема,
антивирус и пр.
А в этом углу,
у нас Дэйв!!

Социальная инженерия - психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации

Вся суть проблем в ИБ

- Использование человеческого фактора
- Просто, эффективно и очень опасно
- Дешево и сердито
- ТОП-3 наиболее популярных методов атак 2017 года



Social Engineering

Атаку социального инженера можно разбить на основные этапы:

- Сбор информации о целевом объекте
- Подготовка сценария действий и необходимых средств атаки (фишинговые ресурсы, вредоносные вложения и др.)
- Установление связей и завоевание доверия жертвы
- Достижение цели атаки (получение необходимой информации)

Атака начинается со сбора информации о целевом объекте (здесь и далее будем иметь в виду атаку не на физическое лицо, а на компанию). Например, будет полезна такая информация:

- списки имен и должностей сотрудников
- адреса электронной почты, номера мобильных телефонов сотрудников, внутренние телефонные номера
- внутренняя структура организации
- архитектура вычислительной сети организации
- используемые технические средства и программно-аппаратное обеспечение
- терминология и принятый жаргон
- информация о конкурентах, партнерах и клиентах компании

Social Engineering



16:12
Mail Delivery System <noreply@[REDACTED]
Fw: Список на увольнение 12.2017

Кому:

Увольнения 2017-2018.docm
495 KB

From: Mail Delivery System <[noreply@\[REDACTED\]](mailto:noreply@[REDACTED])
Date: 2017/12/19
Subject: Mail delivery failed: returning message to sender

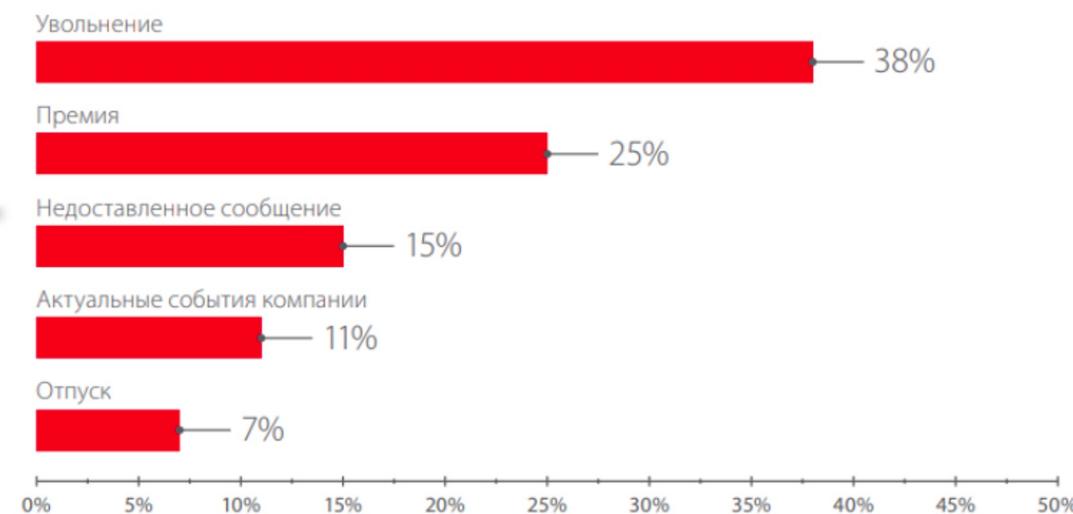
This message was created automatically by mail delivery software.

A message that you sent could not be delivered to one or more of its recipients. This is a permanent error. The following address(es) failed:

SMTP error from remote mailer after RCPT TO: "Human Resources" <[hr@\[REDACTED\]](mailto:hr@[REDACTED])>
50 Requested action not taken:
mailbox unavailable

----- This is a copy of the message, including all the headers. -----

Темы тестовых писем (доля успешных сценариев)



Social Engineering

Развитие атаки с вектором «социальная инженерия»



От: mail@mail.ru
Дата: 21 ноября 2005 г. 11:54
Кому: [admin@mail.ru](#)
Тема: Администрация M@il.ru

Добрый день.

В связи с проблемами, возникшими на нашем сервере, DNS сервер перезагрузился, чем вызвал сбой в работе MySQL базы данных. Возникла проблема с отправкой и получением писем через Web интерфейс. Просим вас выслать на наш резервный адрес: dnsserver@mail.ru пароль вашей почты для восстановления нормальной работы прокси клиента.

Надеемся на ваше понимание администрация M@mail.ru

Кому:  [REDACTED]
Дополнительный оплачиваемый отпуск

Сообщение [Заявление на компенсацию.csv \(4 Кбайт\)](#)

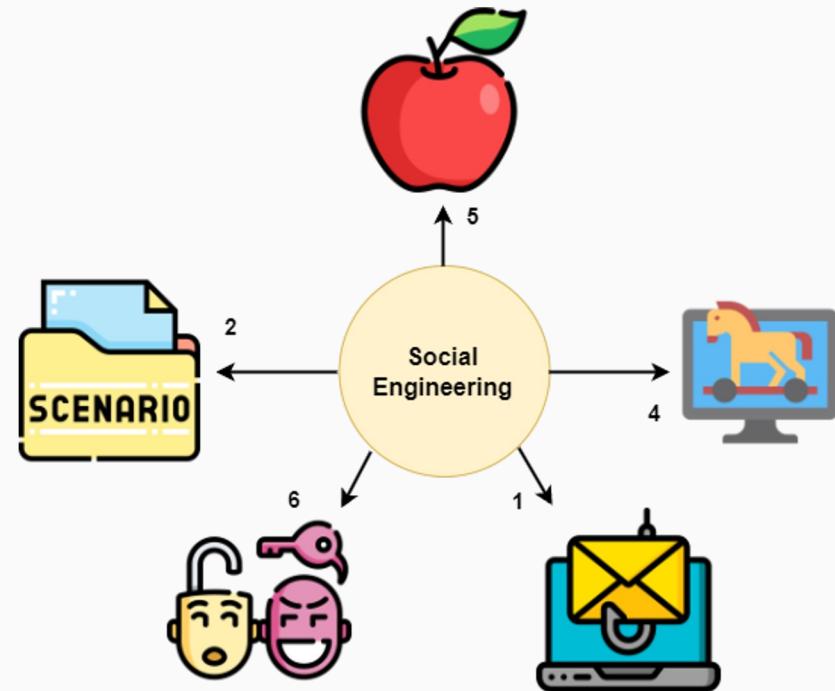
Уважаемые сотрудники,

Напоминаем вам, что вы можете написать заявление на компенсацию неиспользованного дополнительного оплачиваемого отпуска.
Вам будут компенсированы все дни, накопившиеся на конец.
Заявление на компенсацию доступно по ссылке и во вложении: <https://mail.ru/php?id=17374>
Просим обратить пристальное внимание на указанные даты в Вашем заявлении.

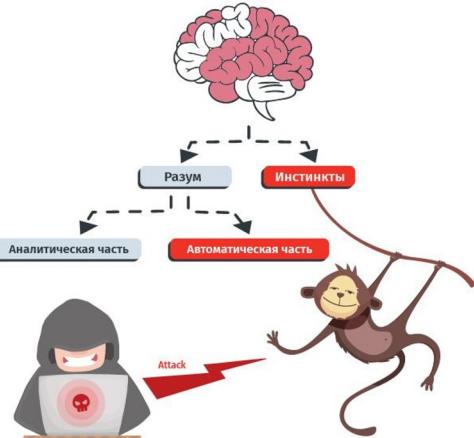
С уважением,

Social Engineering

- 1.Фишинг
- 2.[Претекстинг](#)
- 3.Кви про кво
- 4.Троянский конь
- 5.Дорожное яблоко
- 6.Обратная социальная инженерия.



Обратная социальная инженерия - ситуация при которой жертва сама обращается к злоумышленнику с целью передать закрытую информацию.



Чтобы снизить риск успешной атаки на человеческие ресурсы фирмы, **необходимо научить людей находить подозрительные маркеры** и разработать четкие правила работы с информацией.

Необходимо составить и внедрить инструкции по общению с клиентами и в целом вне компании.

Инструкции по работе с информацией. Необходимо обучать людей цифровой гигиене и в целом безопасности.

Повышение осведомленности. Для уменьшения возможности применения уязвимостей в общении и различных тактик.

Чтение литературы, для развития навыков в сфере цифровой гигиены безопасности.

Social Engineering Как защититься?

- Остерегайтесь незнакомых телефонных номеров с которых Вам звонят .
- Запросите номер телефона звонящего, уточните его ФИО и должность (если он представился сотрудником Банка) Вам человека и записав его, сообщите, что Вы перезвоните позже ему .
- Проверьте принадлежность номера телефона через сеть интернет . Чтобы подтвердить личность звонящих Вам людей, найдите альтернативный номер телефона организации, от которой звонят . Свяжитесь с представителем организацией напрямую по найденному номеру .
- Не перезванивайте по номеру телефона, который вам дали неизвестные люди (этот номер может быть подставным номером телефона) .
- Правонарушители обладают изначально базовой информацией о Вас . Будьте бдительны и не думайте, что если звонящий раскрывает минимальную информацию о Вас, то он действительно является сотрудником фирмы от имени которой якобы звонит .

Информационная безопасность и социальная инженерия

Аудит информационной безопасности:

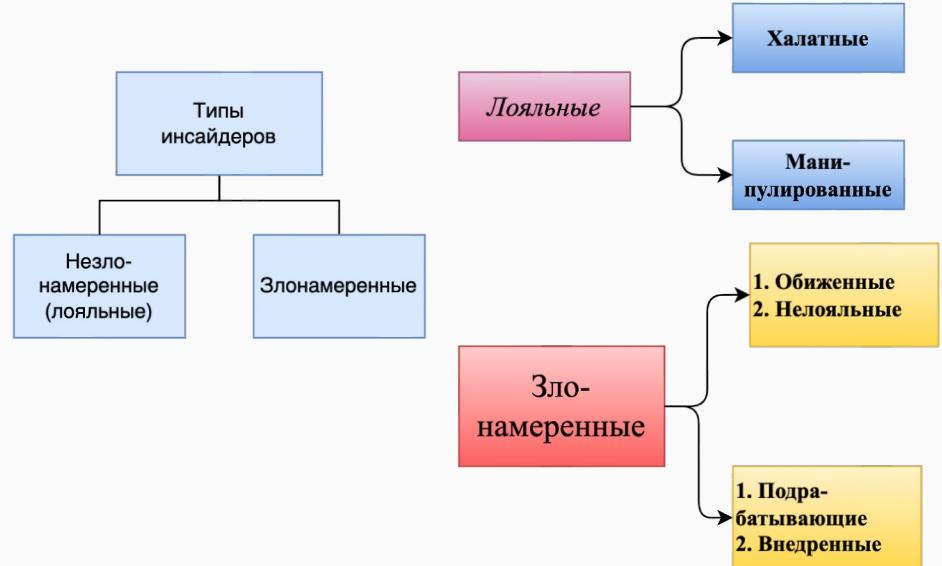
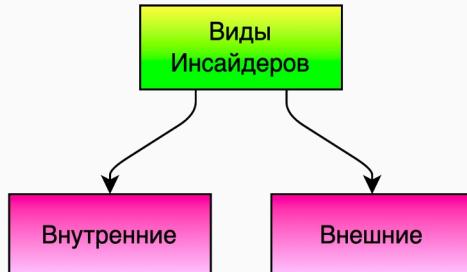
- Проверка возможности получения доступа к конфиденциальной информации
- Проверка возможности получения доступа к информационным системам (в том числе, физического)
- Проверка эффективности работы IDS/IPS, DLP и прочих СЗИ
- Проверка работы служб информационной и внутренней безопасности
- Проверка осведомлённости сотрудников в вопросах ИБ

Инсайдеры#1

В январе 20 года было проведено закрытое заседание об опасности коронавируса для экономики.

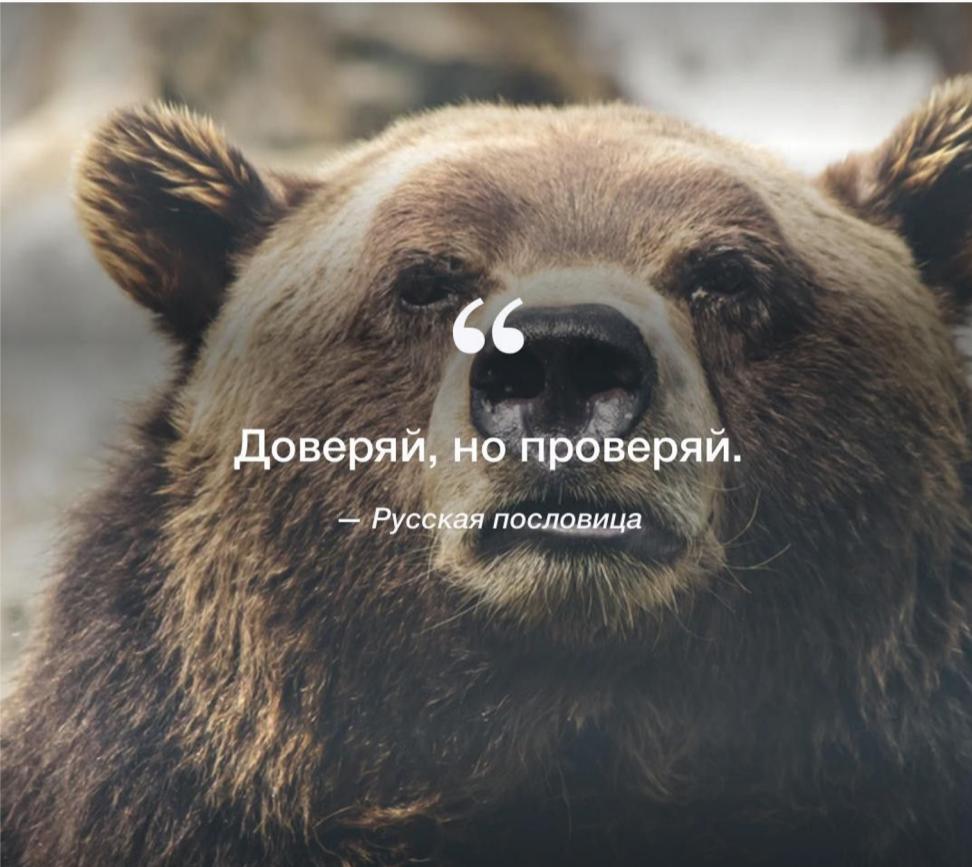
После этого некоторые сенаторы, продали ценные бумаги на сумму более 1 млн долларов.

Позже Министерство юстиции проверяло эти сделки на предмет инсайдерской торговли, но вину сенаторов не доказали.



Инсайдер - член какой-либо группы людей, имеющей доступ к информации, недоступной широкой публике

[Подробная информация](#)



“
Доверяй, но проверяй.

— Русская пословица

Американцы на луне
Чипирование, иллюминаты и массоны
оружие массового поражения
Много чего интересного о COVID-19



Распознайте фейк — чек-лист!

- Источники анонимные, вымышленные или вообще отсутствуют
- Много эмоциональных слов, но мало конкретики
- Новости нет в авторитетных медиа или других источниках
- Копирование одного и того же текста в соцсетях
- Аккаунты, распространяющие новость, не похожи на живых людей
- Новость предлагает конспирологическое объяснение событий
- Новость провоцирует конфликт



Псевдо-фишинговые письма друзьям...

1. [Gophish](#) – фишинговый инструмент
2. [SEToolkit](#) – фреймворк для социальной инженерии
3. [Shellphish](#) – набор фишинговых страниц
4. [HiddenEye](#) – инструмент для фишинга
5. [King-Phisher](#) – инструмент для имитации фишинга
6. [BlackEye](#) – инструмент для фишинга
7. [Evilginx2](#) – фрэймворк для MITM

Разослать фишинговое письмо с уникальной информацией, ведущее на копию крупного ресурса (соцсети, почты и т.д.)

Иван Петрович Лобан 35 лет не женат, есть двое детей.

Информация о субъекте:

Работник газовой сферы,
активно использует соцсети,
увлекается охотой,
состоит в книжном клубе
путешествует по миру посещая рабочие конференции.
Сын – 10 лет, ходит в школу, зовут Иван
Дочь – 5 лет, посещает подготовительную группу.

saamkrolik@gmail.com

