Обеспечение информационной безопасности компьютерных сетей

Презентация подготвленна студентами группы №104: Подгайным Владимиром, Калашниковой Евгенией и

Компьютерная сеть

- Компьютерная сеть (вычислительная сеть) — система, обеспечивающая обмен данными между вычислительными устройствами.

  Для передачи информации могут быть использованы различные среды. Самые распространённые и известные из них:

  •LAN

  •WAN

Обеспечение безопасности в компьютерных сетях

Информационный ресурс корпоративного уровня особенно уязвим и требует надежной защиты.

В современном глобальном мире сетевая безопасность имеет решающее значение. Предприятиям необходимо обеспечивать безопасный доступ для сотрудников к сетевым ресурсам в любое время, для чего современная стратегия обеспечения сетевой безопасности должна учитывать ряд таких факторов, как увеличение надежности сети, эффективное управление безопасностью и защиту от постоянно эволюционирующих угроз и новых методов атак.

Сетевая безопасность

- Из всего вышесказанного напрашивается простой вывод – в современном мире нельзя игнорировать вопросы информационной безопасности; в ответ на новые угрозы нужно искать новые подходы к реализации стратегии защиты информации, а так же использовать новые методы и средства обеспечения сетевой безопасности.

Методы мошенников

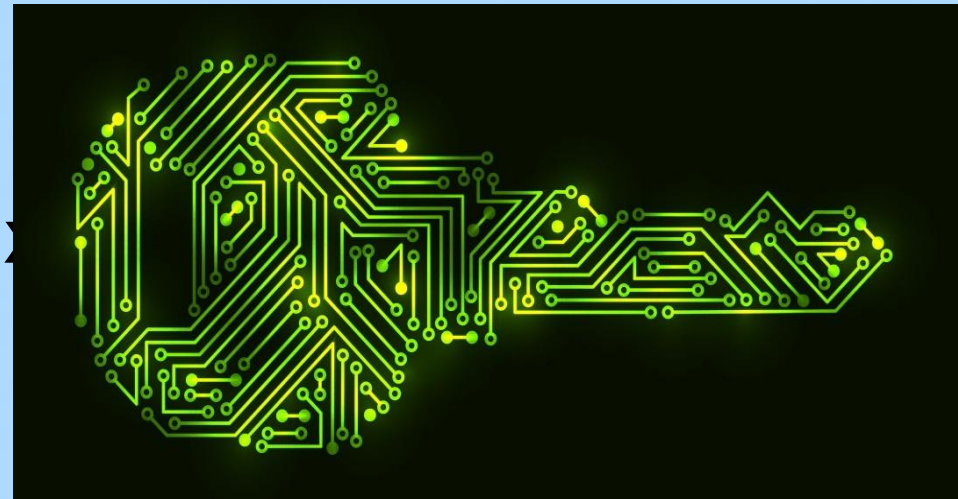
Сегодня интернет стал самым универсальным сервисом, облегчающим жизнь человечеству. С помощью интернета можно сделать многое, если человек хочет заработать или потратить деньги, найти себе развлечение или обменяться мыслями с другими людьми, ему поможет интернет. Однако в то же время как он смог разнообразить нашу жизнь, так он её и ограничил.

В сети полно мошенников, которые хотят облегчить чужой кошелёк. При этом количество методов обмана в интернет-сети просто ошеломляет.

Прежде всего, вы должны быть внимательны. По сути, внимательность – это единственное, что может вас спасти от предложений мошенников. И еще «узнать волка» поможет знание популярных методов обмана в интернете.

Приемы обмана пользователя

- Зачастую мошенники являются хорошими психологами. Они отлично знают человеческие слабости и умело их используют.
- Мошенники вбиваются в доверие, а потом в случае «несчастного инцидента», просят скинуть какую-либо сумму.
- Мошенники, занимаются кражей паролей и личных данных



Технологии на службе злоумышленников

- 1. Вредоносное программное обеспечение
  2. Создание поддельных сайтов
  3. Переадресация запросов (фарминг)
  4. Использование технических возможностей популярных интернет-ресурсов: например, системы рассылки сообщений друзьям в социальных сетях.

Данные и средства

- Многие пользователи не подозревают, что рискуют распространением личных тайн и конфиденциальной информации. Безопасность и защита информации – то, о чем задумываются лишь немногие. Люди, использующие ПК, не защищают важные налоговые и банковские сведения. Стоит помнить, что в процессе работы в Интернете хакеры легко могут завладеть ценной информацией на носителе и уничтожить её.

  Объектами атак хакеров становятся не только государственные учреждения, банки или популярные сайты. Личная информация рядовых пользователей тоже может заинтересовать взломщиков.

Методы защиты информации

1. Физические средства защиты информации. К ним относятся ограничение или полный запрет доступа посторонних лиц на территорию.

2. Базовые средства защиты электронной информации. К ним относятся многочисленные антивирусные программы, а также системы фильтрации электронной почты.

3. Резервное копирование данных. Это решение, подразумевающее хранение важной информации на конкретном устройстве (ПК, телефон)

4. План аварийного восстановления данных. Крайняя мера защиты информации после потери данных. Такой план необходим каждой компании.

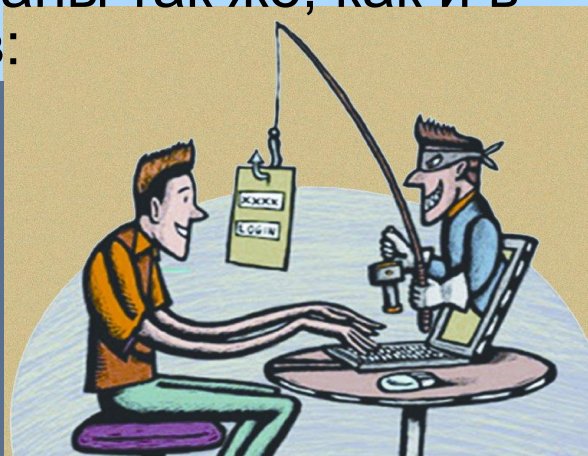
Если стали жертвой мошенников в интернете

Мошенничество – это похищение имущества. При этом не имеет значения, как именно было совершено подобное противоправное действие. Это значит, что если у вас украли деньги или иные ценности через интернет, это такое же уголовное преступление, как и совершенное в реальной жизни.

Однако, несмотря на одинаковые признаки и состав деяния, привлечь к ответственности виртуальных мошенников сложнее. Связано это с отсутствием личного контакта и достаточных сведений о личности. Тем не менее, найти сетевых воров и привлечь их к ответственности все же можно, если действовать правильно.

Если вы стали жертвой виртуальных мошенников, заявление об этом подается в правоохранительные органы так же, как и в стандартной ситуации. Обращаться можно в:

- Полицию.
- Прокуратуру.




Спасибо за внимание!