Единый урок безопасности в сети Интернет

Учитель информатики и ИКТ
Меджидова Юлия Калабеговна
МБОУ «Николаевская СОШ»

СОДЕРЖАНИЕ

ОБЩАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

В наши дни интернет стал неотъемлемой частью нашей жизни.

С его помощью мы получаем информацию, общаемся, обмениваемся данными, оплачиваем товары и услуги, отправляем документы для поступления в вузы и делаем многое другое.

Вместе с тем интернет таит в себе опасности — о них необходимо знать, чтобы избегать их.

WI-FI СЕТИ

УГРОЗЫ:

- Перехват данных - это одна из самых популярных угроз. База или хот-споты Wi-Fi подобны радиоприемнику, который принимает сигнал с данными. Это означает, что с помощью другого приемного устройства и специальных программ-сканеров можно также принимать и расшифровывать информацию. Именно этим и занимаются злоумышленники;
- Wi-Fi ловушки. Ты нашел сеть без пароля и подключился через нее к интернету. В это время владелец точки осуществляет с помощью специальных программ запись всего трафика;
- Существуют специальные программы, с помощью которых злоумышленники могут получить доступ к твоему аккаунту в социальной сети;
- Подмена точек раздач с помощью другого имени точки, где установлены программы по контролю за твоим устройством;
- Взлом сети. Злоумышленники могут найти ошибки в работе алгоритма и расшифровать данные.

СОВЕТЫ ПО БЕЗОПАСНОСТИ

- Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера. Чтобы сделать что-то важное, нужно воспользоваться более защищенными источниками сети;
- Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
- При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
- В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

ONLINE ИГРЫ

УГРОЗЫ

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Заполучив пароль, злоумышленник автоматически приобретает полный контроль над твоим персонажем и его имуществом. Похищенные ценности он может присвоить себе, потребовать у игрока выкуп или выставить на аукцион для продажи, а твои деньги перевести на другой счет.

Так исторически получилось, что любая игровая ценность имеет денежный эквивалент: у популярных игр даже есть свой своя виртуальная валюта, а для торгов уже существуют несколько десятков сайтов по всему интернету.

Однако кроме непосредственно кражи денег со счета очень часто преступников привлекают сами персонажи. Например, высокоуровневые герои из World of Warcraft стоят от 2 до 20 тысяч рублей на сайте торгов героями из этой игры.

СОВЕТЫ ПО БЕЗОПАСНОСТИ АККАУНТА

- Будьте в курсе классификаций и возрастных ограничений в игре.
- Не указывайте личную информацию в профайле игры. Таким образом, другие игроки не смогут Вас найти и Вы будете в безопасности.
- Используй сложные и разные пароли.
- Даже во время игры не стоит отключать антивирус. Пока Вы играете, Ваш компьютер могут заразить.
- Остерегайтесь игр в социальных сетях. Когда Вы даете доступ к Вашему профилю, Вы даете злоумышленникам шанс получить Ваши личные данные.

КИБЕРБУЛЛИНГ ИЛИ ВИРТУАЛЬНОЕ ИЗДЕВАТЕЛЬСТВО

Единый урок безопасности в сети Интернет
МБОУ "Николаевская СОШ"

РАЗНОВИДНОСТИ

- **Флейм** (от английского «flame») или виртуальная перепалка. Обмен эмоциональными репликами в открытом доступе. Вначале все воспринимается как активное обсуждение, но оно может зайти дальше и нанести человеку психологический вред.
- **Атаки**. Буллинг по сотовой связи сводится к отправке жертве повторяющихся оскорбительных сообщений или звонков. На форумах и в чатах преследователи понижают авторитет жертвы, если такая форма ранга предусмотрена на форуме.Оказывают давление в обсуждениях, реагируют на сообщения жертвы унижающими и оскорбительными сообщениями и совместным обсуждением реальных и мнимых недостатков жертвы. Обычно этим занимается целая группа преследователей. В online играх преследователи играют не ради победы, а с целью понизить игровой опыт жертвы целенаправленным давлением.
- **Клевета**. Распространение оскорбительной и неправдивой информации в виде фото, сообщений, песен. Нередко это может быть не отдельная жертва, а целая группа подростков, которые попадают под критику и шутки одноклассников.
- **Самозванство**. Преследователь представляется жертвой или, используя доступ к ее аккаунту, или создавая фейк (фальшивый аккаунт). От имени жертвы распространяет в блогах, социальных сетях и системах мгновенных сообщений негативную информацию, провоцируя окружающих на конфликт с жертвой.

- **Распространение закрытой информации**. Получив конфиденциальную информацию о жертве, преследователь передает ее тому, кому она не предназначалась, вызывая конфликт.
- **Изоляция**. Любому человеку присуще желание быть частью общества (класса, группы подростков во дворе, в сообществе в социальной сети). Ощущение себя частью сообщества является необходимой потребностью каждого человека, как физиологические потребности в пище, воздухе и потребность в самореализации. Изоляция человека от общества наносит серьезную травму человеку.
  Формы изоляции в киберпространстве могут быть разными, начиная от создания закрытого сообщества до игнорирования сообщений жертвы.
- **Киберпреследование**. Скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т. д.
- **Хеппислепинг** («Happy Slapping» с английского «счастливое похлопывание»). Заключается в избиении жертвы и с записью этого на видео, с последующим выкладыванием ролика в сети.

СОВЕТЫ

- Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт. Кроме того, преследователь только и ждет, когда ты выйдешь из равновесия.
- Управляй своей киберрепутацией.
- Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом. Так что в случае нанесения реального вреда, найти злоумышленника можно.
- Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.
- Соблюдай свой виртуальную честь смолоду.
- Храни подтверждения фактов нападений. Если тебя расстроило сообщение, картинка, видео и т.д. обратись за помощью и советом к родителям. Сохрани или распечатай страницу.

- Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии. Лучший защита от нападения – игнор.
- Если ты свидетель кибер-буллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.
- Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.
- Не стоит игнорировать агрессивные сообщения, если они содержат угрозы, особенн систематические. Следует скопировать эти сообщения и обратиться в правоохранительные органы. По поводу размещения оскорбительной информации, размещенной на сайте, следует обратиться к администратору с требованием ее удаления.

КОМПЬЮТЕРНЫЕ ВИРУСЫ

ОСНОВНЫЕ ВИДЫ ВИРУСОВ И ИХ ОПИСАНИЕ

Троянская программа - вредоносная программа, проникающая на компьютер под видом безвредной.

Может:

- Мешать работе пользователя
- Шпионить за пользователем
- Использовать ресурсы компьютера для какой-либо незаконной деятельности и т.д.

Spyware (шпионское программное обеспечение) - программа, которая скрытным образом устанавливается на компьютер с целью полного или частичного контроля за работой компьютера.

Может:

- Собирать информацию о привычках пользования Интернетом и наиболее часто посещаемых сайтах.
- Запоминать нажатия клавиш на клавиатуре, записывать скриншоты экрана и в дальнейшем отправлять информацию создателю spyware;
- Несанкционированно и удалённо управлять компьютером;
- Устанавливать на компьютер дополнительные программы;
- Изменять параметры операционной системы;
- Перенаправлять тебя в браузерах на сайты, которые заражены другими вирусами.

Сетевой червь - разновидность самовоспроизводящихся компьютерных программ, распространяющихся в локальных и глобальных компьютерных сетях. Червь является самостоятельной программой.

Руткит (Rootkit) - программа или набор программ, использующих технологии

сокрытия системных объектов (файлов,

процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр) посредством обхода механизмов защиты системы.

Признаки заражения этим вирусом:

- Вывод на экран странных сообщений или изображений;
- Подача странных звуковых сигналов;
- Неожиданное открытие и закрытие лотка CD и DVD -ROM устройства;
- Произвольный, без твоего участия, запуск на компьютере каких-либо программ.

МЕТОДЫ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ

- Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
- Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
- Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
- Ограничь физический доступ к компьютеру для посторонних лиц;
- Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проференных источников;
- Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их .

МОБИЛЬНЫЙ ТЕЛЕФОН

Злоумышленника может заинтересовать следующее:

ДОСТУП К ПОЧТОВОМУ ЯЩИКУ

- Многие, как только берут свой смартфон в руки, сразу вбивают свои данные и делают доступ к своей электронной почте с мобильного телефона. Да, это удобно, однако, если твой мобильный телефон взломают или ты его потеряешь, то преступники получат доступ к твоему почтовому ящику, а если он твой основной почтовый ящик, то они смогут получить доступ к любому твоему профилю.
- Также они могут получить доступ ко всей твоей переписке, а также ко всем сервисам, привязанным к почтовому ящику. Кроме этого они могут рассылать от твоего имени спам и зараженные файлы твоим знакомым.

ИНТЕРНЕТ-МЕССЕНДЖЕР

- Благодаря интернет-технологиям и смартфонам очень популярна стала интернет-телефония типа Skype и обмен мгновенными сообщениями типа ICQ. Твой профиль, деньги, твои контакты и вся переписка могут оказать в руках чужих людей, которым нельзя доверять. Кроме этого они могут рассылать от твоего имени спам и зараженные файлы твоим знакомым.

ДОКУМЕНТЫ И ЗАМЕТКИ

- За последние несколько лет появилось огромное количество приложений, предназначенных для работы с документами и заметками. Емкость памяти телефона уже превышает обычную флешку, что не ограничивает тебя в добавлении и ведении новых документов. Но эти документы могут тебе очень сильно навредить, если они попадут злоумышленникам, они могут тебя скомпрометировать.
- Также некоторые люди используют подобные сервисы для хранения паролей, что дает злоумышленникам дополнительную выгоду от получения твоего телефона.

ДЕНЬГИ НА ТВОЕМ СЧЕТУ

- Одной из главной целью может стать счет твоего номера телефона. Злоумышленники могут получить к нему доступ, и через специальные схемы вывести с твоего счета все деньги и вогнать тебя в долги перед оператором связи.
- Примером может стать подключение без твоего ведома услуги, за которую будут сниматься деньги с твоего счета. Данная схема может работать постоянно, а главное ты не будешь понимать, куда уходят твои деньги.

BLUETOOTH

- Bluetooth - это быстрый и удобный способ обмена контентом - фотографиями, музыкой и другими файлами. Но важно знать, что когда ты включаешь свой Bluetooth, то люди, находящиеся поблизости, могут получить доступ к файлам в твоем телефоне и к твоим контактам.
- Также, кроме потери личной информации из телефона, сам телефон после заражения или повреждения может потерять свою производительность.

СОВЕТЫ ПО ЗАЩИТЕ

- Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.
- Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
- Подумай, прежде чем нажимать на кнопку «Загрузить». Не открывай мультимедийные сообщения (MMS) и вложения в сообщениях электронной почты и SMS. Они могут содержать вредоносное программное обеспечение и перевести тебя на вредоносный веб-сайт.
- Необходимо обновлять операционную систему твоего смартфона. Это можно сделать через настройки или через приложения по закачке какого-то контента, например через AppleStore или через AndroidMarket
- Существуют версии антивирусных программ для мобильных телефонов. Используй их для сохранения безопасности телефона.
- Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.
- После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.
- Также если у тебя на телефоне хранится много важной и личной информации, типа личных фотографий, то скачивай их на компьютер или перенеси их на диск.
- Периодически проверяй у оператора связи какие платные услуги активированы на твоем номере.

ФОТОКАМЕРА НА ТЕЛЕФОНЕ

- Подумай дважды перед тем, как сделать снимок на свой мобильный телефон. Тебе действительно это нужно сделать?
- Если ты сделал «не хорошую» фотографию, то ни с кем ею не делись. Это может быть очень заманчивым, но подумай о том, как это будет выглядеть со стороны и к чему это может привести.
- Подумай о том, могут ли твои действия унизить кого-то? Избегай фотографирования и видеосъемки других людей без их разрешения. Это может иметь серьезные юридические последствия для тебя.

BLUETOOTH

- Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.
- Если ты используешь bluetooth, то измени настройки так, чтобы телефон был «невидимый», а также установи пароль для доступа.
- Устройство bluetooth должно быть блокировано или не видно окружающим.
- Измени пароль по умолчанию, чтобы окружающие не знали имени устройства, и не смогли идентифицировать тебя и модель телефона.

ПОКУПКИ В ИНТЕРНЕТЕ

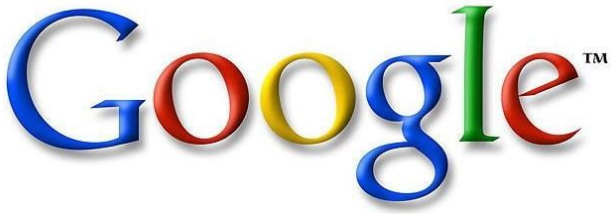
Способы, которые используют злоумышленники для получения доступа к счетам:

- Перевод по Western Union. Данный вид перевода применим только между частными лицами, нет возможности отзыва или опротестования платежа.
- «Обычные» SMS-платежи на короткий номер с неизменяемой суммой. Нет возможности отзыва или опротестования платежа. Маленькие суммы, отсутствие квитанций. По причине своей простоты часто используется в различных мошеннических схемах, и обычно не применяется серьёзными интернет-магазинами, работающими, как говорилось выше, через специализированные платежные системы.

СОВЕТЫ ПО ЗАЩИТЕ

- Используй авторитетные и устоявшиеся в интернете сайты
- Используй сайты, которые находятся в юриспруденции российского законодательства. Международные сайты могут не регулироваться нашими законами, поэтому риски увеличиваются, так как у тебя не будет защиты от государства.
- Перед заказом, необходимо точно знать цену, условия приобретения чего-либо, условия доставки и гарантийные условия. Если это не указано в анкете, то лучше всего будет лично связаться с продавцом и задать ему вопросы.
- Читай на сайте интернет-магазина соглашение о конфиденциальности.
- Убедись в возможности подать жалобу или/и отменить заказ.
- Когда вводишь свои личные данные желательно, чтобы в адресной строке браузера появился значок ключа. Это означает, что соединение безопасно и твои данные не будут украдены.
- На сайте магазина должен быть адрес, номер телефона или электронная почта для связи в случае возникновения вопросов.
- Попытайся найти сертификаты сторонних организаций. Компании могут размещать эти сертификаты, если они соблюдают ряд жестких стандартов, которые определяют методы их работы.

ГИД ПО RUNET



ПОЧТА MAIL.RU

Настройки, которые помогут сохранить безопасность аккаунта:

- Изменить пароль.
- Привязать аккаунт к мобильному телефону.
- Добавить дополнительный e-mail
- Использовать специальные настройки безопасности
- Использовать "безопасное соединение" (HTTPS)

OPERA

Функции безопастности

- Автообновления
- Настройка cookie
- Установка мастер-пароля
- Блокируемое содержимое
- Защита от мошенничества

GOOGLE

Функция безопасного поиска - "Фильтр Безопасного поиска Google"

- Включая такой фильтр, ты практически полностью ограждаешь себя от мата и порнографии в результатах поиска.
- Как это сделать?
- Посети страницу настроек.
- В разделе "Безопасный поиск" выбери уровень защиты.
- Строгая фильтрация – убирает из результатов поиска Google не только видео и изображения сексуального характера, но и ссылки на подобные материалы.
  Умеренная фильтрация – убирает из результатов поиска Google видео и изображения сексуального характера, но не затрагивает ссылки на подобные материалы. Этот параметр Безопасного поиска задан по умолчанию.
  Не применять фильтр к результатам поиска – полное отключение фильтров Безопасного поиска.
- Указав требуемый уровень безопасности, нажми внизу экрана кнопку "Сохранить настройки".

ПОИСК ЯНДЕКСА

Функция безопасного поиска - «Семейный поиск»

- Включая в настройках поиска режим «Семейный поиск» на компьютере, ты практически полностью ограждаешь себя от мата и порнографии в результатах поиска. Воспользоваться интерфейсом «Семейного поиска» без использования настроек можно по адресу family.yandex.ru.
- Сам сайт не изменяется, меняется только выдача результатов в поиске.

ЛИТЕРАТУРА

- http://www.apkpro.ru/content/blogcategory/34/113/