

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ



КОМПЬЮТЕРНЫЕ ВИРУСЫ

- Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю.



МЕТОДЫ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ:

- Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- Ограничь физический доступ к компьютеру для посторонних лиц;
 - Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
- Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
 - Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

СЕТИ WI-FI

- Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WESA», что обозначало словосочетание «Wireless Fidelity», который переводится как «беспроводная точность». До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi»



СОВЕТЫ ПО БЕЗОПАСНОСТИ РАБОТЕ В ОБЩЕДОСТУПНЫХ СЕТЯХ WI-FI:

- Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
- 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;
- Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
- В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

СОЦИАЛЬНЫЕ СЕТИ

- Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

The Facebook logo, featuring the word "facebook" in white lowercase letters on a blue background with a white outline, set against a black background.

facebook



ОСНОВНЫЕ СОВЕТЫ ПО БЕЗОПАСНОСТИ В СОЦИАЛЬНЫХ СЕТЯХ:

- Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
 - Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
 - Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
 - Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
 - Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
 - При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
 - Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

КИБЕРБУЛЛИНГ ИЛИ ВИРТУАЛЬНОЕ ИЗДЕВАТЕЛЬСТВО

- Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.



ОСНОВНЫЕ СОВЕТЫ ПО БОРЬБЕ С КИБЕРБУЛЛИНГОМ:

- Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
 - Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
- Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
 - Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;

ONLINE ИГРЫ .

- Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.



ОСНОВНЫЕ СОВЕТЫ ПО БЕЗОПАСНОСТИ ТВОЕГО ИГРОВОГО АККАУНТА:

- Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
 - Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
 - Не указывай личную информацию в профайле игры;
 - Уважай других участников по игре;
 - Не устанавливай неофициальные патчи и моды;
 - Используй сложные и разные пароли;
 - Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

- Скачать материал целиком можно бесплатно по ссылке внизу страницы.

- **ВСЕРОССИЙСКИЙ**
- **УРОК БЕЗОПАСНОСТИ**
- **ШКОЛЬНИКОВ В СЕТИ**
- **ИНТЕРНЕТ**

- подготовила и провела:

- Подповедная С.А.

- **Тема: Единый урок «Безопасный Интернет»**

- **Цель урока:**

- Познакомить учащихся с преимуществами сети Интернет, скрытыми и открытыми угрозами Интернета, классификации интернет угроз;

- Сформировать понятия Интернета; Научить учащихся критически относиться к информационной продукции, распространяемой в сети Интернет; Уметь отличать достоверные сведения от недостоверных, вредную информацию от безопасной; Распознавать признаки злоупотребления неопытностью и доверчивостью учащихся, попытки вовлечения их в противоправную деятельность.

- **Оборудование:** интерактивная доска с ноутбуком, презентация, видео ролик, буклеты, смайлики.

- **Ход урока:**

- 1. Организационный момент (приветствие учащихся начальной школы, основной и средней школы).

- 2. Мотивационное начало урока

- Тема нашего урока "Безопасность в Интернете"



ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА ЯВЛЯЕТСЯ БЕЗОПАСНЫМ, ЕСЛИ СОБЛЮДАЮТСЯ 3 ОСНОВНЫХ ПРАВИЛА.

1. Защитите свой компьютер.

Регулярно обновляйте операционную систему. Используйте антивирусную программу. Создавайте резервные копии важных файлов. Будьте осторожны при загрузке содержимого.

2. Защитите себя в Интернете.

С осторожностью разглашайте личную информацию. Думайте о том, с кем говорите.

Помните, что в Интернете не вся информация надежна и не все пользователи откровенны.

3. Соблюдайте правила.

Закону необходимо подчиняться даже в Интернете.

При работе в Интернете не забывайте заботиться об остальных так же, как о себе

