Информационная памятка для обучающихся

С каждым годом молодежи в интернете становится больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

Компьютерные вирусы

Компьютерный вирус – это разновидность компьютерных программ, отличительной способностью которых является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случае распространения вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьезный уровень защиты от вредоносных программ;
2. Постоянно устанавливай пачти (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;
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не пользователя большинству вредоносных программ инсталлироваться на твоём персональном компьютере;
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничь физический доступ к компьютеру для посторонних лиц;

6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из профессиональных источников;
7. Не открывай компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он их тебе.

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 «WEGA» , что обозначала словосочетание «Wireless Fidelity», который переводится как «беспроводная точность».

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «WI-FI». Такое название было дано с намеком на стандарт высший звуковой техники HI-FI, что в переводе означает «высокая точность».

Да, бесплатный интернет – доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные *WI-FI*-сети не являются безопасными.

Советы по безопасности работе в общедоступных сетях **WI-FI:**

1. Не передавай свою личную информацию через общедоступные WI-FI сети. Работай в них, желательно не вводить пароли доступа, логины и какие то номера.
2. Используй и обновляй антивирусные программы и брандмауэр. Тем самым ты обезопасишь себя от закачки вируса на твоё устройство;

3. 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 учёбе;

4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту.

5. Используй только защищенное стекло соединение через HTTPS, а не HTTP, то есть при наборе веб-адреса вводи именно «http://»;

6. 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 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.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
2. 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;
3. 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;

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информацию: имя, место жительства, место учебы и прочее;
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твоё местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ к одному, а не во все сразу.

Электронные деньги

Электронные деньги - это очень удобный способ платежей, однако существует мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в зако