

## Информационная памятка для несовершеннолетних по вопросам кибербезопасности в сети «Интернет»

### Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению (копированию). 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 случаев распространяются вирусы через интернет.

#### **Методы защиты от вредоносных программ:**

1. Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
2. 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;
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ устанавливаться 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 проверенных источников;
7. 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

С помощью WI-Fi можно получить бесплатный интернет-доступ в общественных местах: кафе, отелях, торговых центрах и аэропортах. Так же является отличной возможностью выхода в Интернет. Но многие эксперты считают, что общедоступные WiFi сети не являются безопасными.

#### **Советы по безопасности работы в общедоступных сетях Wi-fi**

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая 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 учебе;

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

5. Используй только защищенное соединение через HTTPS, а не т.е. при наборе веб-адреса вводи именно «https://»;

6. В мобильном телефоне отключи функцию «Подключение к сетям автоматически». Не допускай автоматического подключения устройства к сетям без твоего согласия.

### Социальные сети

Социальная сеть - это сайт, который предоставляет возможность осуществлять общение между собой в интернете. Чаще всего в них для каждого человека выделяется своя личная страничка, на которой он указывает различную информацию, начиная от имени, фамилии и заканчивая личными фотографиями. Многие пользователи не понимают, что информация, размещённая ими в социальных сетях, может быть найдена и использована кем угодно, причём не обязательно с благими намерениями.

#### **Основные советы по безопасности в социальных сетях:**

1. Ограничь список друзей. У тебя в друзьях не должно быть случаев знакомых людей;
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, дату твоего рождения и другую личную информацию. Злоумышленники используют 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? Не публикуй что-то до публикации, написать и загрузить;
4. Если ты говоришь с людьми, которых не знаешь, не используй реальное имя и другую личную информацию: имя, место жительства, место учебы;
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 только к одному месту, а не во все сразу.

### Электронные деньги

Электронные деньги — это очень удобный способ платежей, существуют 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 законах.

В России же они функционируют и о них уже прописано в законе, разделяют на несколько видов - анонимные и не анонимные. Разница в том, анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в не анонимных идентификация пользователя является обязательной.