**Методы защиты от вредоносных программ:**

* Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
* Постоянно устанавливай пачти (цифровые заплатки, которые автоматически устанавливаются с целью дорабтки 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.

**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;
* 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;
* Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
* Ипользуй только защищенное соединение через HTTPS, а не НТТР, т.е. при наборе веб-адреса вводи именно «https://»;
* В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

**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.

**Основные советы по безопасной работе с электронной почтой:**

* Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
* Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный\_фанат@» или «рок2013» вместо «тема13»;
* Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
* Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
* Если есть возможность написать самому свой личный вопрос, используй эту возможность;
* Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
* Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;

После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».