**ПАМЯТКА**

**для учащихся по безопасности в сети Интернет**



**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;
* Используй 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».

**Основные советы для безопасности мобильного телефона:**

* Ничего не является по-настоящему бесплатным. 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?
* Необходимо обновлять операционную систему твоего смартфона;
* Используй антивирусные программы для мобильных телефонов;
* 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;
* Периодически проверяй какие платные услуги активированы на твоем номере;
* Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
* Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

**Цифровая репутация**  
*Цифровая репутация*- это негативная или позитивная информация в сети о тебе. Компрометирующая информация размещенная в интернете может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети.   
  
Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.   
  
Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

**Основные советы по защите цифровой репутации:**

* Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
* В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
* Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

