**Памятка родителям по обеспечению безопасности школьников**

**в сети Интернет**

***Советы по безопасности работе в общедоступных сетях Wi-fi:***

**- не передавать личную информацию через общедоступные Wi-Fi сети, работая в них, желательно не вводить пароли доступа, логины и какие-то номера;**

**- использовать и систематически обновлять антивирусные программы;**

**- при использовании Wi-Fi отключить функцию «Общий доступ к файлам и принтерам»;**

**- использовать только защищенное соединение; при наборе веб-адреса вводи «https://».**

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

**- ограничить список друзей; он не должен включать случайных и незнакомых людей;**

**- защитить свою частную жизнь; не указывать пароли, телефоны, адреса и другую личную информацию;**

**- защитить свою репутацию;подумай, прежде чем что-то опубликовать, написать и загрузить;**

**- старайся не разглашать свое реальное имя и другую личную информацию в разговоре с незнакомыми людьми;**

**- избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;**

**- используй сложные пароли при регистрации в социальной сети;**

**- используй различные пароли для социальной сети, почты и других сайтов и в этом случае возможные злоумышленники получат доступ только к одной информации, а не ко всем сразу.**

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

**- выбери правильный почтовый сервис;**

**- не указывай в личной почте информацию о себе;**

**- выбери сложный, надежный, устойчивый пароль для каждого почтового ящика;**

**- используй несколько почтовых ящиков и первый среди них для частной переписки с адресатами, которым ты доверяешь (этот адрес не стоит использовать при регистрации на форумах и сайтах);**

**- не открывай неизвестные файлы, уточни у друзей отправку писем к вам.**

***Основные советы для безопасности мобильного телефона:***

**- будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;**

**- подумай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?**

**- не загружай приложения от неизвестного источника, они могут содержать вредоносное программное обеспечение;**

**- сообщай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;**

**- bluetooth должен быть выключен, когда ты им не пользуешься.**

***Основные советы по борьбе с фишингом (интернет-мошенничеством, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей).***

**- cледи за своим аккаунтом, если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;**

**- используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;**

**- используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в Сети, а не ко всем;**

**- если тебя взломали, то необходимо предупредить всех своих знакомых, которых ты добавил в друзья, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;**

**- 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.**

***Основные советы по защите цифровой репутации:***

**– Цифровая репутация - это негативная или позитивная информация в Сети о тебе. Компрометирующая информация размещенная в Интернете может серьезным образом отразиться на твоей реальной жизни. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в Сети. 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.**

**- 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**