**Информационная памятка для обучающихся**

Школьники - это одни из самых активных пользователей интернета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

**Компьютерные вирусы**  
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 инсталлироваться на твоем 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**  
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 брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое 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. Ипользуй только защищенное соединение через HTTPS, а не 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**  
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 информации: имя, место жительства, место учебы и прочее;  
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое 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**  
1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;  
2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;  
3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и  символы. Например, StROng!;;  
4. Не вводи свои личные данные на сайтах, которым не доверяешь.

**Электронная почта**  
1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;  
2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный\_фанат@» или «рок2013» вместо «темаІЗ»;  
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;  
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;  
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;  
6. 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;  
7. 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;  
8. После окончания работы на почтовом сервисе не забудь нажать кнопку «Выйти».

**Кибербуллинг или виртуальное издевательство**  
1. Не бросайся в бой. Успокойся. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;  
2. Управляй своей киберрепутацией;  
3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;  
4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;  
5. Соблюдай свой виртуальную честь смолоду;  
6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;  
7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;  
8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

**Мобильный телефон**  
1. Ничего не является по-настоящему бесплатным. Будь осторожен, когда тебе предлагают бесплатный контент. В нем могут быть скрыты какие-либо платные услуги;  
2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?  
3. Необходимо обновлять операционную систему твоего смартфона;  
4. Используй антивирусные программы для мобильных телефонов;  
5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;  
6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;  
7. Периодически проверяй какие платные услуги активированы на твоем номере;  
8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;  
9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

**Online игры**  
1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;  
2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;  
3. Не указывай личную информацию в профайле игры;  
4. Уважай других участников по игре;  
5. Не устанавливай неофициальные патчи и моды;  
6. Используй сложные и разные пароли;  
7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

**Фишинг или кража личных данных**  
1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;  
2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;  
3. 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;  
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;  
5. Установи надежный пароль (PIN) на мобильный телефон;  
6. Отключи сохранение пароля в браузере;  
7. 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.

**Цифровая репутация**  
Цифровая репутация - это негативная или позитивная информация в сети о тебе. Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Комментарии, размещение 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. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на престижную и высокооплачиваемую работу. Основные советы по защите цифровой репутации:  
1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;  
2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;  
3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

**Авторское право**  
Современные школьники - активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения авторских прав. Авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/ творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/ исполнять в эфире или размещать в Интернете. Использование «пиратского» программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства. Не стоит также забывать, что существуют легальные бесплатные программы, которые можно найти в сети.