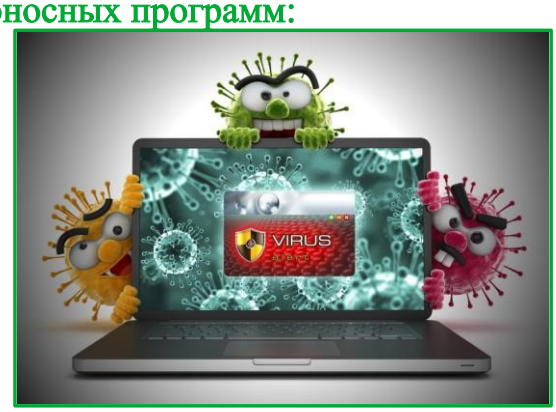
Памятка по безопасности в Интернете

С каждым годом молодежи в интернете становиться больше, а дети школьного возраста одни из самых активных пользователей Internet. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь безопасно находиться в сети.

Компьютерные вирусы

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. 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:



- Используйте современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- Постоянно устанавливайте патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивайте их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включите его;
- Работайте на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на персональном компьютере;
- Используйте антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
- Ограничьте физический доступ к компьютеру для посторонних лиц;
- Используйте внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;

- Не открывайте компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал ваш знакомый. Лучше уточни у него, отправлял ли он их вам.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «Wireless Fidelity», который переводится как «беспроводная точность». До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высший звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Советы по безопасности работе в общедоступных сетях Wi-fi: Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;

- Используйте и обновляйте антивирусные программы и брандмауер. Тем самым вы обезопасите себя от закачки вируса на ваше устройство;
- При использовании Wi-Fi отключите 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 используйте публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
- Используйте только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
- В мобильном телефоне отключите функцию «Подключение к WiFi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без вашего согласия.

Социальные сети Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что

является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

- Ограничьте список друзей. У вас в друзьях не должно быть случайных и незнакомых людей;
- Защищайте свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату вашего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как вы и ваши родители планируете провести каникулы;
- Защищайте свою репутацию - держите ее в чистоте и задавай себе вопрос: хотели бы вы, чтобы другие пользователи видели, что вы загружаете? Подумайте, прежде чем что-то опубликовать, написать и загрузить;
- Если вы говорите с людьми, которых не знаете, не используйте свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- Избегайте размещение фотографий в Интернете, где вы изображены на местности, по которой можно определить ваше 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 вас взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги — это очень удобный способ платежей, однако 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. Электронные деньги разделяют на несколько видов – анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в не анонимных идентификации пользователя является обязательной. Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

- Привяжите к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудете свой платежный пароль или зайдете на сайт с незнакомого устройства;
- Используйте одноразовые пароли. После перехода на усиленную авторизацию вам уже не будет угрожать опасность кражи или перехвата платежного пароля;

Выберите 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 несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;

Не вводите свои личные данные на сайтах, которым не доверяете.

Электронная почта

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

- Надо выбирайте правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
- Не указывайте 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;
- Выберите 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;
- Используйте несколько почтовых ящиков. Первый для частной переписки с адресатами, которым вы доверяете. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;

- Не открывайте файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточните у них, отправляли ли они вам эти файлы;
- После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

Кибербуллинг или виртуальное издевательство

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов. **Основные советы по борьбе с кибербуллингом:**

- Не бросайтесь в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться.

Если начать отвечать оскорблениями на оскорбления, то только еще больше усугубится конфликт;

- Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
- Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все действия и сохраняет их. Удалить их будет крайне затруднительно;
- Игнорируйте единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
- Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
- Если вы свидетель кибербуллинга. Ваши действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддерживайте жертву, которой нужна психологическая помощь.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные

аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

- Ничего не является по-настоящему бесплатным. Будьте осторожны, ведь когда вам предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
- Думайте, прежде чем отправить SMS, фото или видео. Вы точно знаете, где они будут в конечном итоге?
- Необходимо обновлять операционную систему вашего смартфона;
- Используйте антивирусные программы для мобильных телефонов;
- Не загружайте приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
- После того как вы выйдете с сайта, где вводили личную информацию, зайди в настройки браузера и удалите cookies;

Периодически проверяй какие платные услуги активированы на вашем номере;

- Давайте свой номер мобильного телефона только людям, которых вы знаете и кому доверяете;
- Bluetooth должен быть выключен, когда вы им не пользуетесь. Не забывайте иногда проверять это.

Online игры

Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр. **Основные советы по безопасности твоего игрового аккаунта:**

- Если другой игрок ведет себя плохо или создает вам неприятности, заблокируй его в списке игроков;
- Пожалуйтесь администраторам игры на плохое поведение этого игрока, желательно приложить доказательства в виде скринов;
- Не указывайте личную информацию в профайле игры;
- Уважайте других участников по игре;
- Не устанавливайте неофициальные патчи и моды;
- Используйте сложные и разные пароли;
- Даже во время игры не стоит отключать антивирус. Пока вы играете, ваш компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься «любимым» делом. Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля). **Основные советы по борьбе с фишингом:**

- Следите за своим аккаунтом. Если вы подозреваете, что ваша анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
- Используйте безопасные веб-сайты, в том числе, интернетмагазинов и поисковых систем;
- Используйте сложные и разные пароли. Таким образом, если вас взломают, то злоумышленники получат доступ только к одному вашему профилю в сети, а не ко всем;
- Если вас взломали, то необходимо предупредить всех своих знакомых, которые добавлены у вас в друзьях, о том, что вас взломали и, возможно, от вашего имени будет рассылаться спам и ссылки на фишинговые сайты;
- Установите надежный пароль (PIN) на мобильный телефон;

- Отключите сохранение пароля в браузере;
- Не открывайте файлы и другие вложения в письмах даже если они пришли от ваших друзей. Лучше уточните у них, отправляли ли они вам эти файлы.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о вас.

Компрометирующая информация размещенная в интернете может серьезным образом отразиться на вашей реальной жизни. «Цифровая репутация» - это ваш имидж, который формируется из информации о вас в интернете. Ваше место жительства, учебы, 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. Вы даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять вас на работу.

Комментарии, размещение ваших фотографий и другие действия могут не исчезнуть даже после того, как вы их удалите. Вы не знаете, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о вас 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:

Подумайте, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;

- В настройках профиля установите ограничения на просмотр вашего профиля и его содержимого, сделай его только «для друзей»;
- Не размещайте и не указывайте 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 прав на интеллектуальную собственность.

Термин «интеллектуальная собственность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги , и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

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 вашим аккаунтам до блокировки вашего устройства, где установлена не легальная программа. Не стоит также забывать, что существует легальные и бесплатные программы, которые можно найти в сети.