

Информационная памятка педагогам по безопасности в сети интернет

старший воспитатель Норенко Н. В.

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

- 1. Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- 2. Постоянно устанавливай пачти (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 твоём 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



- Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WESA», 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

- 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 загрузки вируса на твоё 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. Используй только защищённое соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
- 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



- 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

- 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.

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

- 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 «тема13»;
- 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 перед закрытием вкладки с сайтом не забудь нажать на «Выйти».



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

- 1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то 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.
-

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, password — пароль).



Основные советы по борьбе с фишингом

- 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. 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 окружающие 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

- 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.

Сетевичок.рф



- Сетевичок.рф — интернет-портал для обучения детей и подростков основам кибербезопасности. Создан при поддержке Лиги безопасного интернета, Министерства образования и науки РФ и Госдумы ФС РФ. Эксперты сервиса в режиме онлайн помогают пользователям решить различные проблемы, связанные с пребыванием в глобальной сети. Устраивают всевозможные конкурсы для учащихся школ всех возрастных групп (от 7 до 18 лет). Публикуют обзоры лучших веб-сайтов.