Памятка для педагогов о безопасности в сети Интернет

Пользователей интернета с каждым годом становится все больше. Между тем, помимо огромного количества возможностей, Интернет несет и проблемы. Эта памятка поможет Вам 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 зараженная программа, а также повредить или 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 серьезный уровень защиты от вредоносных программ.
- Постоянно устанавливайте патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления операционной системы. Скачивайте их только с официального сайта разработчика операционной системы. Если существует режим автоматического обновления, включите его.
- Работайте на своем компьютере под правами пользователя, а не администратора. Это позволит большинству вредоносных программ удалиться с персонального компьютера.
- 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 или диск только из проверенных источников.
- На вскрывайте компьютерные файлы, полученные из ненадежных источников. Даже те файлы, которые присланы от знакомого. Лучше уточните у него, отправлял ли он их Вам.

Сети WI-FI

WI-FI – это не вид передачи данных, не технология, а всего лишь бренд. Еще в 1991 году нидерландская компания зарегистрировала бренд «WEGA», что обозначило словосочетание, которое 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 звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Бесплатный интернет-доступ в кафе, отелях является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные сети WI-FI не являются безопасными.

Советы по безопасности работы 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. 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 активирую ее для удобства использования в работе.
- Не используйте публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту.
- Используйте только защищенное соединение, то есть при наборе веб-адреса вводите именно «https://».
- В мобильном телефоне отключите функцию «Подключение к WI-FI автоматически». Не допускайте 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. 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. Желательно, чтобы у Вас в друзьях не было случайных и незнакомых людей.
- Защищайте свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату своего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как Вы планируете провести отпуск.
- Защищайте свою репутацию – держите ее в чистоте и задавайте себе вопрос: хотели бы Вы, чтобы другие пользователи видели, что вы загружаете?
- Подумайте прежде, чем что-то опубликовать или загрузить.
- Избегайте размещения фотографий с 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 Вашу страницу взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги – это способ платежей, однако существуют мошенники, которые хотят получить эти деньги. В России об электронных деньгах прописано в законе, где их 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 неанонимных – идентификация 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 безопасность 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.
- 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 передачи файла.

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 знаете и кто первый в рейтинге.

✓ Не указывайте в почте личную информацию.

✓ Используйте двухэтапную авторизацию. 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, используйте эту возможность.

✓ Используйте несколько потовых ящиков. Первый для частной переписки с адресами, которым Вы доверяете. Этот электронный адрес не надо использовать при регистрации на форумах и сайтах.

✓ 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.

✓ После окончания работы на почтовом сервисе перед закрытием вкладки с сайтам не забудьте нажать на «Выйти».

Кибербуллинг или виртуальное издевательство

Кибербуллинг – преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство, социальное бойкотирование помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

- Не бросайтесь в бой. сли Вы начнете отвечать оскорблениями на оскорбления, то только еще больше разожжете конфликт.
- Управляйте своей киберрепутацией.
- Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.
- Интернет фиксирует все Ваши действия и сохраняет их.
- Игнорируйте единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.
- 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, поддерживать жертву, которой нужна психологическая помощь.

Мобильный телефон

Средств защиты современных смартфонов очень мало. 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.

✓ Необходимо обновлять операционную систему своего смартфона.

✓ Используйте антивирусные программы для мобильных телефонов.

✓ Не загружайте приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.

✓ После того как Вы выйдите с сайта, где вводили личную информацию, зайдите в настройки браузера и удалите cookies.

✓ Bluetooth должен быть выключен, когда вы им не пользуетесь. Не забывайте иногда проверять это.

Фишинг или кража личных данных

Главная цель интернет-мошенничества или фишинга состоит в получении конфиденциальных данных пользователей – логинов и паролей.

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, интернет-магазинов 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 ваших знакомых, которые добавлены у Вас в друзья, о том, что вас взломали и, возможно, от Вашего имени будет рассылаться спам и ссылки на фишинговые сайты.
- Установите надежный пароль на мобильный телефон.
- Отключите сохранение пароля в браузере.
- Не открывайте подозрительные файлы и другие вложения в письмах даже если они пришли от знакомых Вам людей. Лучше уточните у них, отправляли ли они Вам эти файлы.

Цифровая репутация

Цифровая репутация – это позитивная или негативная 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.

Многие люди легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий.

Комментарии, размещенные под Вашими фотографиями, 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 думают о Вас окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред.

Основные советы по защите цифровой репутации:

- Подумайте, прежде, чем опубликовать что-то опубликовать у себя в социальной сети.
- В настройках профиля установите ограничения на просмотр Вашего профиля и его содержимого.
- Не размещайте и не указывайте информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные педагоги – 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 или 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 использовать его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать 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 нелегальная программа. Не стоит также забывать, что существуют легальные и бесплатные программы, которые можно найти в сети.