Рекомендации о безопасности интернета для обучающихся.

Виды информационных угроз

1. 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:

- используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- 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;
- работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
- используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
- ограничь физический доступ к компьютеру для посторонних лиц;
- используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
- не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

2. 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 безопасной работе в общедоступных сетях Wi-Fi:**

- не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
- используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
- 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;
- не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
- используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
- в мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

3. 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:

- ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
- 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;
- 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;
- если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

- избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое 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 тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

4. Электронные деньги и банковские карты

В Интернете можно осуществлять покупки с банковских карт и с помощью электронных денег.

Электронные деньги - это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Обычно сервисы электронных денег предлагают клиентам анонимные и неанонимные аккаунты. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной. Зачастую анонимные аккаунты имеют существенные ограничения в свой работе и соответственно имеют минимальный уровень безопасности.

Также следует различать электронные фиатные деньги, равные государственным валютам, и электронные нефиатные деньги, которые в свою очередь не равны государственным валютам.

В Интернете можно также расплачиваться банковскими картами, которые обычно разделяют на:
- зарплатные карты. Их открывает банк по указанию предприятия, которое будет осуществлять выплату заработной платы, аванса, премий, отпускных, командировочных, социальных пособий, положенных работнику;
- кредитные карты. Они имеют денежные средства, принадлежащие банку и предоставленные в качестве кредита. Эти деньги предоставляются на определенных условиях и на конкретный срок, в том числе в пределах выделенного лимита;
- дебитовые карты. Они открываются для использования и расчетов собственными средствами. На них не установлено кредитного лимита, поскольку клиенту доступен баланс в размере внесенных им денег.

Важно помнить, что для покупок в Интернете зачастую достаточно знать только номер карты и срок ее действия, чем очень часто и пользуются злоумышленники.

Сервисы электронных денег и банки предоставляют возможность привязки к счету мобильного телефона, что позволяет не только восстановить доступ к счету или карте, а также подтверждать платежи (транзакции) с помощью одноразового пароля.

Основные советы по безопасной работе с электронными деньгами:

- 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;
- используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
- 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 несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;
- Не вводи свои личные данные на сайтах, которым не доверяешь.

Что делать, если:

- потеряна банковская карта. Сообщить по телефону в банк о произошедшем и попросить ее заблокировать. Банк предложит вместо данной карты выпустить новую карту с новым номером. Пока не будет заблокирована банковская карта, любой, у кого она окажется в руках, сможет воспользоваться ею;
- пришло уведомление о платеже, который вы не совершали. Необходимо сообщить в банк или платежный сервис, направив заявление о чарджбеке (отмене операции), в котором максимально подробно описать произошедшее. Банк или платежный сервис рассмотрит обращение и вернет вам деньги в срок от 30 до 60 дней.

Важно помнить, что чем раньше удастся выявить проблему и начать предпринимать меры, то тем больше шансов уменьшить ущерб, который может быть нанесен вам, вашей семье и другим лицам.

5. 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 выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
- не указывай 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;
- выбери 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;
- 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;
- 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;
- после окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

6. 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 бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
- управляй своей киберрепутацией;
- анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
- не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
- соблюдай свою виртуальную честь смолоду;
- игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
- 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.

7. 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. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.

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

Необходимо обновлять операционную систему твоего смартфона.

Используй антивирусные программы для мобильных телефонов.

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

После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.

Периодически проверяй, какие платные услуги активированы на твоем номере

Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

8. 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 тебе неприятности, заблокируй его в списке игроков;
- пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;

- не указывай личную информацию в профайле игры;
- уважай других участников по игре;
- не устанавливай неофициальные патчи и моды;
- используй сложные и разные пароли;
- даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

9. Сетевое мошенничество

С развитием сети интернет его стали осваивать и мошенники. Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги и получить личные и конфиденциальные данные: к таким данным относятся логины и пароли от различных сервисов, в том числе банковских, номера и пин-коды банковских карт и другие персональные данные.

Сетевое мошенничество имеет множество методов.

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) предполагает за счет использования различных методов заманивания пользователя на поддельный сайт, например, через ссылку в письме, баннер или ссылку в тексте.

Иногда вредоносная ссылка маскируется под правильную ссылку – так злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение с помощью опечатки в адресе сайта, или сайты, копирующие интерфейс известных ресурсов. Примеры: http://www.sberbank.ru/ и http://www.sbenbank.ru/ либо www.yandex.ru и www.yadndex.ru.

На подобных сайтах пользователю предлагается ввести логин и пароль или данные счета, после чего зачастую происходит перенаправление на реальный сайт, но данные уже попадают в руки мошенников.

Вишинг является разновидностью фишинга, в которой используется телефон. Мошенник может позвонить и представиться сотрудником банка или платежного сервиса и попросить продиктовать какие-либо платежные данные, например, пароль или код, пришедший на телефон. Его цель – выманить платежные данные, с помощью которых можно украсть деньги с карты или кошелька. Часто дополнительно присылается СМС со ссылкой, которая ведет на фишинговый сайт.

Фарминг или скрытое перенаправление является также разновидностью фишинга, но направляет пользователя вирус или взломанная программа на поддельный сайт, являющийся полной копией официального ресурса.

Сетевое мошенничество имеет также множество видов, в частности:

- липовые акции и фальшивые выигрыши в лотереи. Пользователь может получить сообщение (по телефону, почте или SMS), что выиграл некий приз, а для его получения необходимо «уплатить налог», «оплатить доставку» или просто пополнить какой-то счет;
- признаки фальшивой лотереи: пользователь никогда не принимал участие в лотерее; пользователь никогда не оставлял своих личных данных на этом ресурсе; почтовый адрес отправителя – общедоступный почтовый сервис, например, gmail.com, mail.ru, yandex.ru;
- просьба «друзей» сообщить пароль, когда знакомый в социальной сети сообщает о потере телефона, просит напомнить ваш номер, вам приходит SMS с неким кодом, а тот же друг в социальной сети сообщает, что заказывает товар или регистрируется на сайте и случайно указал ваш телефон вместо своего. Он просит сообщить пришедший код. Таким образом, ваш номер будет подключен к платной подписке и с вас начнут списывать деньги;
- ложная блокировка аккаунта в социальной сети: на баннере подробно расписан вариант «спасения» от блокирования страницы в социальной сети, который включает отправку SMS на «короткий» номер или введение кода подтверждения. В первом случае происходит разовое списание денег, а во втором оформляется ежедневная подписка на какую-либо платную услугу;
- рекламные сообщения и баннеры о необходимости обновления браузера имеют риск подписаться на платную загрузку или получить вирус с архивом платной программы;
- бесплатное скачивание файлов и просмотр каких-либо файлов с подпиской по номеру телефона, после чего включится подписка и с указанного номера могут начать списываться деньги;
- пользователю предлагается бесплатный антивирус, под видом которого на устройство попадет вредоносная программа, либо создается иллюзия, что компьютер уже заражен и для уничтожения угрозы нужно воспользоваться специальным антивирусом, который, опять же, окажется вирусом. Примером является появление надписи на экране компьютера о блокировке операционной системы, устранить которую можно только при отправке SMS с кодом, пришедшим на телефон при подтверждении, – после чего запускается сам вирус;
- предложения очень выгодных покупок, реклама больших скидок или анонс распродаж, которые размещаются на сайтах, в социальных сетях и присылаются СМС или на электронную почту. Такие предложения обычно предполагают перевод денег на банковскую карту, электронный кошелек или мобильный номер. В настоящее время стала актуальна следующая разновидность данной угрозы – пользователям рассылаются на оплату мобильного телефона, домашнего интернета, ЖКХ и т.д.

Зачастую мошенники направляют поддельные квитанции раньше официальной даты оплаты, чтобы успеть собрать свои платежи;

- мошенник может попросить денег в долг под видом знакомого, например, через взломанный аккаунт в социальных сетях. При этом перевести деньги он может попросить любым удобным способом – на электронный кошелек, банковскую карту, через интернет-банк.

Фишинговые сообщения могут содержать:

- сведения, вызывающие тревогу, или угрозы, например, закрытие ваших банковских счетов;
- обещания большой денежной выгоды с минимальными усилиями или вовсе без них;

сведения о сделках, которые слишком хороши для того, чтобы быть правдой;

- запросы о пожертвованиях от лица благотворительных организаций после сообщений в новостях о стихийных бедствиях;
- и другую информацию.

Отдельным подвидом необходимо рассматривать **мобильное мошенничество**, которое в частности предполагает получение СМС-сообщений с незнакомых номеров, которые могут содержать:

- ссылки на фишинговые или зараженные ресурсы;
- информацию о выигрышах, которых не существует;
- ложные просьбы о помощи;
- о переводе денег на сотовый, прямые просьбы о переводе денег;
- SMS из несуществующего банка;
- просьбы перезвонить на платный номер;
- требования выкупа;
- просьбы отправить СМС, которые активируют платные услуги;
- и другую информацию.

Мобильное мошенничество также часто встречается в формах:

Wangiri («Очень дорогой звонок») – когда человек звонит с неизвестного номера, но, как только человек берет трубку, звонок внезапно обрывается. Вы перезваниваете на неизвестный номер и попадаете на автоинформатор, задача которого – как можно дольше удержать абонента на линии, пока со счета списываются деньги.

Требования выкупа – когда вам позвонили или прислали SMS с неизвестного номера с просьбой о помощи близкому человеку: не впадайте в панику, не торопитесь переводить деньги. Перезвоните родным и узнайте, все ли у них в порядке. Уточните, где находятся близкие.

Мобильное мошенничество имеет примеры смежных технологий: пользователю может прийти SMS от банка или платежного сервиса с паролем для совершения платежа, а сразу после этого может позвонить человек, который скажет, что ввел этот номер мобильного телефона по

ошибке и попросит сообщить код из SMS, которое только что пришло пользователю. На самом деле код из SMS — это пароль не к счету незнакомца, а к счету пользователя, с помощью которого злоумышленник может поменять настройки кошелька или интернет-банка, украсть деньги и т.д.

Основные советы по борьбе с фишингом:

- 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;
- используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
- используй сложные и разные пароли. Таким образом, если твой профиль взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
- Если твой профиль взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что возможно от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
- установи надежный пароль (PIN) на мобильный телефон;
- отключи сохранение пароля в браузере;
- 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.

Что делать если уже возникли проблемы?

Если СМС-подписка была оформлена, то необходимо обратиться по телефону в службу поддержки оператора и попросить отключить её.

Если аккаунт был взломан, то необходимо заблокировать аккаунт, сообщить администрации сайта о взломе, поменять пароль к сайту, а также предупредить всех своих знакомых о том, что произошел взлом и, возможно, от вашего имени будет рассылаться спам и ссылки на фишинговые сайты.

Если деньги или другие важные данные вашей банковой карты были предоставлены неизвестным лицам, то необходимо как можно быстрее обратиться в банк для блокировки карты и возврата средств.

10. 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 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:

- 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.

11. 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 ко многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установлена нелегальная программа. Не стоит также забывать, что существует легальные и бесплатные программы, которые можно найти в сети.

Заключение

Необходимо всем помнить, что в настоящее время информационная безопасность – важнейший компонент национальной безопасности, она становится одним из элементов национальной, общественной и личной безопасности.

Для дополнительной информации ты можешь посмотреть мультфильмы на сайте:
Мультфильмы «Безопасный интернет – детям!» (студия Mozga.ru) http://youtu.be/789j0eDglZQ

Информация о безопасности в интернете
http://obo-sosh2.ru/roditelyam/opasnost-interneta.html

ОБЩИЕ РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ ИНТЕРНЕТА И МОБИЛЬНОЙ
СВЯЗИ URL: http://do.znate.ru/docs/index30424.html

Автор – составитель:
Финогенова А.В., заведующий отделом ГУО «Гродненский районный центр творчества детей и молодежи»