ПАМЯТКА по кибербезопасности граждан

Сегодня Интернет-технологии, шагнув далеко вперёд, широко используются в повседневной жизни. В основном, это касается представителей подрастающего поколения, но сейчас с этим приходится сталкиваться и взрослому населению, престарелым гражданам. Между тем, помимо огромного количества полезных возможностей, сеть Интернет несёт в себе и определённую опасность. В связи с этим, немаловажным является предупредить пользователей глобальной сети Интернет о том, какую именно опасность может нести «всемирная паутина» и какие действия нужно предпринимать, чтобы общение с Интернетом оставило только положительные эмоции.

Помимо того, что существуют различные компьютерные вирусы и вредоносные программы, которые необходимо блокировать антивирусными программами, важно помнить и о соблюдении ряда основных правил работы в сети Интернет и, в частности, в социальных сетях. Важно знать, что информация, размещённая гражданами в соцсетях, может быть найдена и использована кем угодно, в том числе, и во вред.

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.

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 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.

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 для детей и их родителей следующие:

- предусмотреть для ребёнка наличие на его персональном компьютере «фильтров», блокирующих посещение сайтов, содержащих противоправную информацию, причиняющую вред детской психике (особенно актуально это касаемо исключения фактов распространения так называемой «интернет-педофилии»);

- родителям необходимо регулярно посещать страницы в социальных сетях, принадлежащих их детям, интересоваться у ребёнка, чем он увлечён, с кем общается и на какие темы. В случае обнаружения необычного поведения детей (постоянная тревога, стремление ребёнка уйти от разговора на тему его общения и интересов в сети Интернет) или каких-либо угроз, вымогательства третьим лицами у ребёнка какой-либо информации или фото-видеоматериалов с его участием, необходимо незамедлительно обращаться к психологу и (или) в правоохранительные органы;

- ограничить список лиц со статусом «друзей» в соцсетях. В «друзьях» не должно быть случайных и незнакомых людей;

- защищать свою частную жизнь (репутацию). Не указывать пароли, телефоны, адрес, дату рождения и другую личную информацию. Необходимо помнить, что злоумышленники могут использовать даже информацию о том, как ребёнок или родители планируют провести каникулы;

- избегать размещения фотографий в Интернете, где есть изображения человека на местности, по которой можно определить местоположение;

- при регистрации в социальной сети необходимо использовать сложные пароли, состоящие из множества букв и цифр (с русской или иностранной раскладкой с количеством знаков не менее 8);

- для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если киберпреступники взломают какую либо личную страницу, то они получат доступ только к одному месту, а не ко всем персональным страницам 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. В России же они функционируют и о них уже 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 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:

- 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.

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».

Кибербуллинг или виртуальное издевательств

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 свой виртуальную честь смолоду;

- игнорируй 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 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

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.

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.

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:

- 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 тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;

- 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;

- 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.

Важно также помнить, что комментарии, размещение фотографий и другие действия могут не исчезнуть даже после того, как будут удалены с личной интернет-страницы. Неизвестно, кто успел сохранить эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что могут подумать окружающее люди, которые найдут и увидят какие-либо компрометирующие сведения. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред.

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.

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

«Скимминг»

На банкоматах или POS-терминалах в торговых точках мошенники могут устанавливать специальные устройства, которые считывают данные с банковских карт. Эта махинация связана и с последующим изготовлением мошенниками дубликатов банковских карт, которые, в комплекте с PIN-кодом, позволяют снять деньги с вашего счета. Для защиты от скимминга банкиры рекомендуют использовать карточки только в тех местах, которые заслуживают доверия и охраняются.

Вирусы, работающие с системами онлайн-банкинга

На ваш компьютер определенным образом попадает вредоносное программное обеспечение. И когда вы пытаетесь зайти в свой аккаунт в платежной системе, вводя одноразовые пароли — эта программа выдает вам сообщение о якобы устаревшем пароле. И каждый следующий код тоже оказывается якобы «устаревшим». Для защиты эксперты рекомендуют постоянно контролировать карточный счёт, подключать к нему смс-банкинг, не оставлять персональные данные о себе и своей карточке на интернет-сайтах, регулярно обновлять антивирусную

защиту, особенно с функцией безопасных платежей.

Программа-вымогатель

Вирус может зашифровать файлы на вашем компьютере, заблокировать ваш доступ к нему, или к любой онлайн-системе, в которой вы зарегистрированы. На экране вы будете видеть только картинку-блокер, и требование заплатить выкуп для того, чтобы расшифровать или разблокировать систему. Например, такие:

- «Отправьте SMS на короткий номер»;

- «Переведите деньги на мобильный счет»;

- «Расплатитесь биткоинами (электронными деньгами)».

Чтобы не «подхватить» вредоносное программное обеспечение такого вида, рекомендуется никогда не «кликать» по ссылкам на сайты банков или других финорганизаций. Надо вводить адрес вручную, иначе есть риск, что вы можете попасть на поддельную страницу, которая выглядит точно так же, как и оригинал.

Таким образом, при работе в сети Интернет важна, прежде всего, предусмотрительность, контроль за близкими людьми (детьми, престарелыми родственниками) и самоконтроль.

Профилактика киберпреступности

Технический прогресс не стоит на месте. Попробуйте поспорить с тем, что современный человек без информационных сетей и виртуального общения уже не представляет собственную жизнь. Скорее всего, Вы поймете, что сами являетесь частью информационного пространства, где вместе с Вами пребывают родные, друзья, коллеги и миллиарды незнакомых людей. И если в добропорядочности близких мы уверены, то предположить, что на уме у незнакомца, невозможно.

Преступления против жизни и здоровья человека, собственности, государственной власти сегодня совершаются с использованием информационных технологий. Поэтому вопросы профилактики киберпреступности являются ключевыми для правоохранительных органов как Российской Федерации, так всего мира. В таких условиях повышается роль участия каждого пользователя сети Интернет в формировании безопасного информационного пространства. Для этого необходимо еще раз соблюдать следующие рекомендации.

- используйте лицензионное программное обеспечение. В таком случае отсутствует риск заразить компьютер или мобильное устройство при установке неизвестной программы.
- установите антивирусную программу и файрволлы не только на персональный

компьютер, но и на смартфон и планшет.

- не переходите по ссылкам, содержащимся в спаме и других подозрительных письмах. При работе с электронными почтовыми ящиками необходимо настроить автоматическое блокирование приходящего спама, а также механически сортировать корреспонденцию, своевременно удаляя подозрительные письма без их просмотра.
- аккаунты в социальных сетях, как и электронные почтовые ящики, периодически подвергаются хакерским атакам, поэтому необходимо минимизировать передачу персональных данных в электронном виде, особенно не указывать логины и пароли мобильного банка, электронных кошельков, номера, пароли и коды банковских карт.
- воздержитесь от покупок на малоизвестных и подозрительных интернет-сайтах и у лиц, осуществляющих продажу товаров или услуг в социальных сетях, особенно при необходимости внесения полной предоплаты за товар или услуги.
- используйте сложные пароли, состоящие из комбинаций цифр и букв или иных символов. Воздержитесь от паролей - дат рождения, имен, фамилий, то есть тех, которые легко вычислить либо подобрать.

Кроме того необходимо обезопасить и ограничить пребывание в сети пользователей, которые не готовы к угрозам безопасности. Как правило, это лица, не имеющие навыков использования информационного пространства – дети и лица пожилого возраста. Установление контролирующих программ и использование конкретных приложений вместо выхода в открытое Интернет-пространство позволят снизить риски заражения компьютера случайным переходом по вирусной ссылке или загрузкой фишинг-страницы.

Почему так сложно расследовать киберпреступления?

1) чрезвычайно высокая латентность киберпреступлений (подавляющее большинство незаконных деяний в сфере высоких технологий остаются не только не раскрытыми, но и даже не учтенными);

2) нередко особо крупные размеры ущерба;

3) транснациональность (прозрачность национальных границ для преступников);

4) высокопрофессиональный состав лиц, совершающих подобные преступления;

5) тенденция к увеличению количества данных преступлений;

6) комплекс юридических и технических проблем, связанных с отсутствием:

- законодательных актов, регулирующих уголовно-процессуальные действия;

- самостоятельно искать доказательства его виновности. Он может лишь проверить и оценить

те доказательства, которые ему представляют сторона обвинения (предварительное следствие) и сторона защиты;

- необходимых технических средств противодействия киберпреступлениям;

- надежной системы взаимодействия с правоохранительными органами зарубежных стран. Специфика борьбы с киберпреступностью состоит в том, что, данные преступления носят интернациональный характер и, в целом, не попадают под юрисдикцию какого-либо конкретного государства.

Серьезную проблему составляет сбор доказательств совершения противоправных действий в телекоммуникационных сетях ввиду легкости уничтожения и изменения компьютерной информации, то есть следов преступления. Невозможности изъятия этих «виртуальных» следов преступления и сложности процессуального оформления, изъятых доказательств, сложности проведения незамедлительных действий, направленных на обнаружение компьютерной информации и идентификации лиц, причастных к преступной деятельности в компьютерных сетях.

В связи с этим, следственное управление Следственного комитета Российской Федерации по Республике Тыва рекомендует гражданам проявлять бдительность, а также соблюдать перечисленные и другие рекомендации по обеспечению безопасной работы в информационной сети Интернет

28 Сентября 2017

Адрес страницы: https://tuva.sledcom.ru/news/item/1167569