Официальный сайт

Следственный комитет
Российской Федерации

Памятка по кибербезопасности

ПАМЯТКА ПО КИБЕРБЕЗОПАСНОСТИ ГРАЖДАН (ПРИ ИСПОЛЬЗОВАНИИ СЕТИ ИНТЕРНЕТ, ЭЛЕКТРОННЫХ БАНКОВСКИХ КАРТ И Т.Д.)

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.

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, причинящую 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 обнаруженя необычного поведения детей (постоянная тревога, стремление ребёнка уйти от разговора на тему его общения и интересов в сети Интернет) или каких-либо угроз, вымогательства третьиим 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. 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);
-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 и использование электронных банковских карт
Электронные деньги - очень удобный способ платежей, однако существуют мошенники, которые могут нажиться на незнании граждан элементарных правил безопасности. Особенно это касается престарелых граждан, пенсионеров.
Основные советы по безопасной работе с электронными деньгами:
-Никогда и никому нельзя сообщать пин-код от собственных электронных банковских карт. Помнить, что вопросы корректности действия банковской карты могут вестись исключительно с представителями банка, выпустившего в оборот эту карту. А для того, чтобы удостовериться, что беседа идет именно с представителями банка, а не с мошенниками, необходимо либо перезванивать в службу поддержки по заранее оговорённым телефонам, либо непосредственно обращаться в специализированные отделения того банка (финансового учреждения), от имени которого выдана банковская карта. Любые приходящие сообщения о блокировке карты и необходимости в связи с этим ввести какой-либо код, пароль, пин-код, всегда должны вызывать настороженность;
-При введении пин-кода на терминале необходимо обеспечить его безопасный ввод, скрывая от посторонних глаз набираемые цифры, стараться снимать денежные средства непосредственно в помещении банка, в местах, где установлены видеокамеры, что (при необходимости) позволит впоследствии выйти на след злоумышленников, наблюдавших за вами и совершающих какие-либо противоправные действия;
-Использовать одноразовые пароли в целях избежания кражи данных или перехвата платёжного пароля;
-Выбирать сложный пароль. Надежные пароли 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.
-Не вводить свои личные данные на подозрительных не проверенных сайтах.

Аналогичные требования можно отнести и к работе с **электронной почтой** (это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети; помимо передачи простого текста, имеется возможность передавать медиафайлы). В частности, не рекомендуется открывать файлы и другие вложения в письмах, даже если они пришли от друзей. Лучше заблаговременно уточнить у них, отправляли ли они указанные файлы.

Работа с мобильным телефоном (смартфоном)
Современные смартфоны и планшеты содержат вполне развитый функционал и могут конкурировать со стационарными компьютерами. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищённость. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.
Основные советы безопасности при пользовнии мобильным телефоном:
-Ничто не является по-настоящему бесплатным. Необходимо быть осторожным, ведь когда предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
-Использовать антивирусные программы для мобильных телефонов;

-Не загружать приложения от неизвестного источника, так как они могут содержать вредоносное программное обеспечение;
-Периодически проверять, какие платные услуги активированы с привязкой к телефонному номеру;
-Предоставлять личный номер мобильного телефона только людям, которых знаешь и кому доверяешь;
-Bluetooth должен быть выключен, когда им не пользуешься.

«Фишинг» или кража личных данных
С развитием интернет-технологий злоумышленники, переместившись в Интернет, создают для граждан новую угрозу: интернет-мошенничество («фишинг»), главная цель которого - в получении конфиденциальных данных пользователей - логинов и паролей. Основные советы по борьбе с «фишингом»:
-Следить за своим аккаунтом. Если есть подозрения, что анкета была взломана, то необходимо заблокировать её и как можно скорее сообщить об этом администраторам ресурса;
-Использовать безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
-Использовать сложные и разные пароли;
-Если взломали личную почту, то необходимо предупредить об этом всех своих знакомых, которые добавлены в «друзьях», и о возможной рассылке от вашего имени спама и ссылок на «фишинговые» сайты;
-Установить надежный пароль (PIN) на мобильный телефон;
-Отключить сохранение пароля в браузере;
-Не открывать файлы и другие вложения в письмах, даже если они пришли от друзей или знакомых. Лучше уточнять у них лично, отправляли ли они указанные 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.

Ещё о кибермошенничестве:

«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 он-лайн-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.

17 Августа 2017 11:41

Адрес страницы: http://sverdlovsk.sledcom.ruhttp://sverdlovsk.sledcom.ru/Pamyatka-po-kiberbezopasnosti

Адрес страницы: http://sverdlovsk.sledcom.ru/Pamyatka-po-kiberbezopasnosti