БУК «Областная библиотека для детей и юношества»

Основы безопасности в Интернете: как избежать угроз

консультация

Л.В. Евсеева, заведующий информационно-библиографическим отделом

В последние годы тема контентной безопасности приобрела исключительную актуальность, в связи, с чем предпринимаются активные шаги по организации информационно-просветительской деятельности, повышающей осведомленность относительно контентных Интернет-опасностей и способствующей профилактике Интернет-угроз.

Консультация предназначена именно для тех случаев, когда специалисту, желающему заниматься информационно-просветительской работой в сфере контентной цифровой безопасности детей и подростков, необходимо самому получить базовое представление о проблеме и ее характеристиках.

Рассмотрим основные контентные угрозы в Интернете, их краткие характеристики, специфику опасности и базовые действия по прекращению оборота этих видов контента. Исходя из кратких описаний Интернет-угроз, можно не только определиться с путями расширения своего кругозора, но и получить базовые навыки по профилактике таких угроз.

Россия сегодня – лидер по времени, проводимому пользователями в социальных сетях. Самыми популярными из них являются: «ВКонтакте», «Одноклассники», «Facebook». Социальные сети «лишают» одиночества и скуки – там всегда есть с кем пообщаться. Внутри социальных сетей создаются профессиональные сообщества и группы по интересам, где можно прочитать немало печатных текстов или прослушать курс лекций, а иногда и найти настоящих реальных друзей. Форумы – площадки, создаваемые для обсуждения какого-то конкретного вопроса, и являющиеся более узким вариантом социальной сети, – позволяют быстро найти ответы на интересующие вопросы.

Совет первый: по обеспечению безопасности в социальных сетях.

- Меньше конкретных данных о своей жизни.
- Не публикуйте информацию, по которой можно определить Ваш домашний адрес и время, когда там никого не бывает.
- Не размещайте в общем доступе посты о дорогостоящих покупках или сделках, в результате которых можно сделать вывод о наличии у Вас крупной суммы денег или ценностей, которые можно перепродать.
- Не описывайте свой постоянный маршрут, пролегающий между домом и работой – нападения с целью ограбления не всегда бывают случайными.

Не секрет**,** что в социальных сетях очень распространен **Троллинг.** Троллинг - это агрессивные, оскорбительные или провокационные комментарии призванные обидеть или разозлить, кого либо, например автора поста. «Сделал гадость – сердцу радость», – тролль пишет, следуя именно этой поговорке. В критике тролля чаще всего нет ни грамма конструктива. В основном тролли – это обезличенные существа (люди), провокаторы, которые питаются человеческими эмоциями. Именно раздражение и огорчение других людей доставляют троллю наибольшую радость. Целью троллинга зачастую является привлечение внимания к себе – тролль хочет почувствовать свою значимость, произвести впечатление, даже если это впечатление резко негативное. Поэтому если чей-либо восторженный «пост» получает негативный, злой комментарий, – это действия злобного тролля. Часто это психически нездоровые люди. Не смотря на вроде бы небольшие масштабы проблемы, тролли могут создавать серьезный дискомфорт при общении в социальных сетях.

Совет второй: как реагировать на троллинг**.**

- Не спорьте с троллем, это бесполезно.
- Игнорируйте тролля, не отвечайте ему и не пытайтесь доказать, что он не прав. Не поддавайтесь искушению ответить троллю «железными аргументами».
- «Не кормить тролля», значит не реагировать эмоционально на его комментарии. Задача тролля не найти истину, а вывести собеседника из себя, поэтому большим разочарованием для него будет молчание в ответ. Можно «забанить» тролля – то есть внести его в личный «черный список» или обратиться к модератору.

При общении в онлайн всегда надо помнить, что под ником может скрываться кто угодно, и приложенные фотографии ничего не значат. Интернет – среда условно анонимная. Условно, потому, что в большинстве случаев вычислить Ваш реальный IP-адрес, то есть сетевой адрес Вашего компьютера, не составляет труда, а оттуда и до адреса офиса Вашего интернет-провайдера совсем недалеко. Но все эти хитрые штуки доступны в основном полицейским, а вот простой пользователь своего собеседника знает только под ником и видит только на фотографиях. Фотография может быть чьей угодно.

Совет третий: о незнакомых друзьях в сети.

- Лучше не добавлять в друзья незнакомых людей.
- Игнорировать пустые аккаунты а также аккаунты без фотографии на аватаре и внутри и аккаунты без человеческого аватара.
- Никогда не приглашать новых «друзей» из Сети к себе домой.
- Если все же очень хочется познакомиться, что называется, «вживую» – лучше встретиться в многолюдном месте.

Хейтер – это яростный противник чего-либо или кого-либо. Слово hater переводится с английского как «ненавистник» и происходит от глагола to hate (ненавидеть). Часто такое лицо осуждает на пустом месте чье-либо творчество, нередко переходит на анализ внешности, личных качеств и даже прямые оскорбления собеседника. Надо помнить, что хейтер – это не критик, поскольку последний в довольно сдержанной манере, аргументировано и без лишних эмоций дает оценку явлению, или человеку, а хейтеру «просто не нравится», «не так, и все». Эти люди могут быть неприязненно настроены люди не лично к собеседнику, а к организации. С ними можно работать, переубеждать, если они не превращаются в троллей.

Совет четвертый: как реагировать на хейтера.

- Попробуйте повернуть отрицательное обсуждение в позитивное русло.
- Постарайтесь снизить накал эмоций.
- Предложите решение проблемы.
- Спросите остались ли вопросы (обычно редко отвечают).
- Ваш комментарий должен быть завершающим. Чаще всего, в 80 процентах это помогает.

Если этот человек отрицательно настроен к лично к Вам, не нравится Ваш блог, Ваше видео, фото, комментарии и прочее, в таком случае:

- Не поддавайтесь на провокации хейтеров.
- Выдохните, успокойтесь.
- Не грубите им.
- Составляйте им ответ в этичной форме, можно послать улыбчивый смайлик.
- Никогда не отвечайте мгновенно, подумайте.
- Чувство юмора спасает в самой безнадежной ситуации.

Не раз Вы встречали цепляющий заголовок или анонс примерно такого содержания: «Вы этому не поверите! Но это работает! Смотреть до конца!», Сенсация!!! Чаще всего люди идут на поводу таких уловок. Подобные заголовки манипулируют чувствами, вводят в заблуждение. Заголовок может преувеличивать детали рассказа или утаивать информацию. Чаще всего используется желтый цвет и много восклицательных знаков. В последнее время в сети появилось много так называемых «фейк» новостных сайтов – сайтов, распространяющих качественно сделанные «ложные» новости. Такого рода новости в интернет могут «вбрасывать» специальные сайты, основным предназначением которых является создание и распространение «фейков». Лженовости могут появляться в результате намеренной попытки распространить «фейк» (главным фактором распространения такого новостного контента является банальная погоня за сенсацией, в результате которой онлайн-издания получают интернет-трафик, клики, внимание пользователей и, как следствие, рост цен на размещаемую

рекламу. В данном случае уместно напомнить пословицу: «Доверяй, но проверяй».

Совет пятый: как реагировать на фейковые новости, желтые заголовки, жареные темы.

- Проверяйте факты, проводите полный обзор информации, ищите ссылки на авторитетные источники.

Еще одна опасность **- кликбейт** – это технология оформления анонсов публикаций таким образом, чтобы на ссылку в самом анонсе нажало как можно больше увидевших его интернет-пользователей. Единственной целью кликбейта является именно высокое соотношение кликов к просмотрам. Происхождение у данного термина, разумеется, англоязычное. И состоит оно из двух слов: click переводится как «щелчок» (то есть тот самый клик кнопкой мышки на ссылку), bait в переводе – «приманка» или «наживка. В социальных сетях, в частности Вконтакте, Одноклассниках очень часто используются кликбейты. Например, в ВК кликбейт – это небольшая история, которая вызывает интерес у пользователей, и которые нажимают ссылку «Читать дальше». Однако после перехода люди сталкиваются с тем, что прежде, чем дочитать интересующий контент, или досмотреть видео, нужно вступить в какое-либо сообщество или совершить другие действия. Таким образом, сообщества с малым количеством подписчиков, не тратя деньги на рекламу, наращивают их число. С помощью техники кликбейта заманиваются пользователи, т.е. данный способ основан на обмане и не удовлетворяет пожелания пользователей.

Лайкбейт (призыв залайкать или прокомментировать публикацию), цель та же, что и у клибейтов т.е. – получение дохода от онлайн-рекламы, особенно в ущерб качеству или точности информации. В некоторых случаях получение дохода не является главной целью, но человеком руководит желание получить как можно больше лайков при оценке фото, или заметки.

Чему еще нельзя доверять в социальных сетях? Обращениям на Ты, если вы не знакомы. Фразам «У меня к тебе просьба…», далее обычно следует пауз, а дальше вымогание денег с помощью просьб, описывания сложной ситуации и пр. Допустим, это знакомый человек, но, возможно произошел взлом страницы Вашего знакомого.

Совет шестой: как предостеречь себя от обмана.

- Если Вас что-то насторожило, перепроверяйте информацию у общих знакомых или позвонив им.
- Спросите у собеседника о каких-либо деталях общения, о которых Ваш собеседник должен знать точно, или попросите подтвердить выдуманный факт.

Токсичная благотворительность – что это? Чаще всего это объявления с просьбой о помощи. Вас могут попросить «перепостить» (разместить у себя на странице в социальной сети) объявление о том, что милый котенок или щенок срочно ищет своего хозяина, его могут усыпить, так как денег на содержание животного нет, а к объявлению прикладывается фото животного и номер телефона его нынешнего владельца. Чаще всего, это попытка мошенническим путём завладеть чужими денежными сбережениями. Например, звонок на указанный номер телефона может оказаться платным. Или на том конце провода поведают слёзную историю, сводящуюся к тому, чтобы забрать питомца, сначала необходимо перечислить / выслать небольшую сумму. А еще возможен современный интернет-вариант липового инвалида, просящего «деньги на лечение», под объявлением которого стоит логотип известного благотворительного фонда, а реквизиты счета не имеют к нему никакого отношения.

Прежде, чем сделать доброе дело, не сразу поддавайтесь на эмоции, мы все живые люди, нам жалко животных, людей, но нужно помнить, о мошенниках. Нужно думать и проверять информацию. Переводить деньги проверенным и хорошо известным благотворительным фондам, брать реквизиты благотворительных организаций на их официальных сайтах, размещать на своей странице в соцсети объявления о требующейся помощи «из первых рук» от людей, которым Вы доверяете.

Совет седьмой: как избежать токсичных благотворителей.

- Не делайте репост просьбы о сборе денег, если вы лично не знаете этого человека. Даже, если это знакомый Вашего знакомого.
- Не становитесь рассыльщиком фейков и спама.
- Не рассылайте сомнительные видео (предупреждения о якобы опасных таблетках и пр.).

Мошенники в e-mail. Сегодня уже мало кто пишет бумажные письма родственникам и друзьям. Есть электронная почта. Сервисов электронной почты очень много, от предоставляемого личным провайдером интернета, до бесплатных «Яндекса» и «Mail.ru». Надо только нажать кнопку «создать почтовый ящик», придумать логин и пароль. Казалось бы, чего проще, но, неприятные неожиданности встречаются и здесь.

Совет восьмой: по созданию электронной почты.

- Придумывайте сложные пароли, не менее 8 символов, в т.ч. заглавные буквы, цифры, знаки. Меняйте пароль сразу, если на почту пришло письмо-предупреждение о входе с незнакомого устройства.
- Старайтесь заводить электронный ящик, используя почтовые сервисы с хорошей степенью фильтрации спама. Например (gmail).

Спам – рассылка электронных писем (чаще рекламы) людям, не выражавшим желания их получать. В общем-то, спам вполне безобидная штука, не приносящая особых неприятностей, кроме раздражения от замусоривания почтового ящика. Тем не менее, спам может быть опасен, важно, что у него внутри. Поэтому, не поленитесь поставить галочку «защита от спама» в настройках Вашего почтового ящика. Или хотя бы отмечайте такие письма – это поможет компьютерной почтовой программе распознавать спам еще на входе и не допускать его попадания в почтовый ящик. Внутренности электронных писем могут содержать «**Трояны» и опасности «бот-нет» - сетей.** Электронная почта отличный способ превратить компьютер в «бот» путем отправки «трояна». **«Бот» (сокращение от «робот»)** – компьютер, зараженный специальной программой, позволяющей злоумышленнику управлять таким компьютером по своему усмотрению без согласия владельца компьютера. Из бот-компьютеров создаются бот-сети (бот-неты), занимающиеся, например, рассылкой спама или атакой на ресурсы банков, и все это при полном неведении хозяев таких компьютеров. **«Троян»** («троянская программа») – вредоносная программа (компьютерный вирус), проникающая на компьютер пользователя под видом безобидного приложения с целью получить доступ к информации, размещенной на компьютере, или возможность удаленно управлять зараженной машиной.

Совет девятый: как избежать спама и других неприятностей.

- Никогда не отвечайте на спам и не переходите по указанным в нем ссылкам – это только даст понять спамерам, что на другом конце живой человек, и спровоцирует новый вал спама.
- Установите плагин для блокировки нежелательных сайтов, рекламы.
- Обязательно установите на компьютер антивирусную программу.
- Не открывайте письма с длинной и непонятной ссылкой. Даже похожей на настоящую, с реального домена.
- Не открывайте письма без темы и неизвестного адреса.
- Не открывайте письма с вложениями архивов или самораспаковывающихся файлов от неизвестных адресов: File.exe, File.zip, File.rar.
- Не открывайте письма с поздравлениями с победой в конкурсе и выйгрышем суперприза (если Вы нигде не участвовали).
- Не открывайте «Нигерийские письма» или «письма счастья».

«**Нигерийские письма» или «письма счастья»** – вид мошенничества, получивший распространение с появлением массовых рассылок писем по электронной почте. Мошенники просят у получателя письма помощи в многомиллионных денежных операциях, обещая солидные проценты от сумм. Если получатель письма, откликнулся и согласился участвовать, оказывается, что для получения «солидного куша» необходимо сделать

самую малость – перевести немного собственных денег на оформление сделки / уплату налогов / взятки чиновникам (нужное подчеркнуть). Кроме этого варианта существует вариант с лотереей – жертве сообщается о крупном выигрыше в лотерею. Получатель письма должен заплатить (например, налог), чтобы получить свой выигрыш. К этому же виду писем относятся письма о получении наследства от почившего богатого дядюшки за рубежом. Их, разумеется, надо сразу отправлять в спам. Также существует онлайн-вариант брачной аферы, в нем мошенники ведут любовную переписку с целью «создания семьи». Суть мошенничества заключается в выманивании относительно небольших сумм «на билет и визу» для встречи с «любимым» или просто на «покупку веб-камеры».

Фишинговые письма. Еще один способ мошенничества при помощи электронной почты – заключается в «выуживании» (по английски fishing – рыбалка) у получателя письма информации, которую потом можно будет «монетизировать», например, адресов электронной почты других пользователей (их можно продать спамерам), паролей от других сервисов (социальных сетей, корпоративной электронной почты и т.д.). На сегодняшний день преобладают фишинговые письма, направленные на получение от пользователя номеров и паролей его кредитных карточек или систем онлайновых платежей. Такие письма обычно маскируются под официальные сообщения от администрации банка, в которых сообщается, что получатель должен подтвердить сведения о себе (или срочно сменить пароль), иначе его счет будет заблокирован. Среди данных, которые необходимо ввести, есть и те, которые нужны мошенникам. Чаще всего отличить «подставной» сайт от официального сайта банка «на глаз» практически нереально. Простому пользователю очень сложно заметить разницу в доменных именах – символах, которые вводятся в адресную строку браузера для попадания на нужную интернет-страничку этих сайтов.

Совет десятый: как не реагировать на «письма счастья».

- Помните, банки или платежные системы никогда не запрашивают конфиденциальную информацию по электронной почте.
- Типичное фишинговое письмо начинается с обезличенного приветствия «Уважаемый пользователь» или обращения по адресу электронной почты. Ваш банк или платежная система обычно знает ФИО адресата и в настоящем письме приветствует собеседника, обращаясь по имени и фамилии (или имени и отчеству). Чаще всего мошеннические электронные письма содержат призывы к безотлагательным действиям (используя такие слова как «немедленно», «безотлагательно», «последнее предупреждение»), пытаясь заставить действовать быстро и необдуманно.
- Не стесняйтесь позвонить в банк по номеру телефона, указанному на Вашей карте (именно на карте, а не указанному в письме или сайте,

открывшемся по ссылке из письма, – там вполне может оказаться человек из команды мошенников) и все уточнить.

- Не пренебрегайте лицензионными антивирусами – многие из них блокируют фишинговые ссылки. Обращайте внимание на любые отклонения от обычного поведения Вашего банка (например, запрос новых сведений, которые раньше не надо было вводить). Если что-то идет не так как обычно, лучше отказаться от операции и перепроверить информацию у банка.
- Не пренебрегайте возможностью услуги «смс-оповещение» от банка – если деньги начнут внезапно утекать с Вашего счета, будет шанс успеть заблокировать карту.

Взлом почты. Здесь важно знать, что если кто-то очень хочет взломать почту, он это сделает. Это вопрос времени и затрат ресурса человеческого или компьютерного (современные хакеры давно автоматизировали процесс взлома – это и быстрее и следов меньше). Как это делается? Подбирается пароль. Это самый простой (и самый используемый) способ вскрытия электронного почтового ящика. Для этого даже не надо быть программистом – в сети гуляет множество программ, которые подставляют в качестве пароля определенные слова (или сочетания символов) используя при этом готовые словари. Подсмотреть пароль, записанный на листочке, может случайно зашедший в гости знакомый человек. Хорошо, если его любопытство ограничится просмотром Ваших фотографий.

Совет одиннадцатый: как избежать взлома почты.

- Не храните в электронном почтовом ящике (особенно на бесплатном почтовом сервисе) ценную информацию, секретные документы и личные фотографии. После пересылки или скачивания обязательно удаляйте такие письма.
- При необходимости переслать ценную для Вас информацию, воспользуйтесь программой шифрования, а код от шифра сообщите собеседнику другим способом, например, по телефону.
- Никто не любит сложных паролей, так как их легко забыть, но если Вы не хотите, чтобы Вашу почту взломали хакеры, то правило - «чем сложнее пароль, тем выше безопасность» – для Вас.
- Если у Вас несколько почтовых ящиков, не используйте на всех один и тот же пароль. Пусть он будет отличаться на 1-2 символа, но это может спасти Вас от утечки всей информации.
- Не ленитесь периодически менять пароли, особенно в случае появления подозрения о том, что текущий вариант пароля скомпрометирован.
- Ни в коем случае не записывайте пароли в блокнотике, который лежит «под рукой» возле монитора компьютера.

- Установите приложение для хранения и генерации надежных паролей. https: // www.lastpass.com/ ru или KeePassXC.
- Храните важные документы в облаке (Я. Диске, Dropbox, Облако Mail, Диск Google), чтобы случайно не удалить, не потерять.

Коммерческие обманы. Чаще всего это происходит, когда мы что-то покупаем в интернет-магазинах. Покупка в интернет-магазине иногда походит на покупку кота в мешке – никогда не знаешь, совпадет ли то, что ты выбрал с тем, что тебе привезут. Чего стоит хотя бы фраза: «Производитель оставляет за собой право изменять конструкцию, технические характеристики, внешний вид, комплектацию товара, не ухудшающие его потребительских качеств, без предварительного уведомления потребителя». Но это, конечно, не самое страшное. Хуже, если Вы останетесь вообще без товара, заплатив при этом какие-то деньги, или вообще без денег. Многие интернет-магазины принимают оплату товара онлайн. Сначала Вы оплачиваете выбранный товар с электронного кошелька (например, через «Яндекс. Деньги») или пластиковой карты, а уже после этого продавец высылает Вам товар. В этом случае самый простой способ обмана покупателя – получив деньги, «скрыться в неизвестном направлении», и интернет позволяет сделать это как нельзя лучше – достаточно просто перестать отвечать на звонки и электронные письма. Другой способ обмана через интернет-магазин – привезти «серый» или заведомо неисправный товар с последующим отказом его ремонтировать или принимать обратно в случае поломки. Некоторое время назад это было достаточно массовое явление для российской интернет-торговли. Онлайн-магазины почему-то считали (а некоторые по-прежнему придерживаются этого подхода к своему бизнесу), что закон «О защите прав потребителей» на них не распространяется, а значит выполнять его не обязательно.

Совет двенадцатый: как избежать коммерческого обмана**.**

- Все же лучше сначала товар, а уж потом деньги.
- По возможности не производите предоплату покупок.
- Большинство российских интернет-магазинов позволяют оплатить товар курьеру после его доставки и проверки.
- Хороший продавец – надежный продавец, покупайте на проверенных сайтах (по рекомендациям знакомых и друзей).
- При покупке из-за рубежа обращайтесь к известным крупным интернет-магазинам («Amazon», «Ebay» и др.) – они дорожат своей репутацией и имеют свою систему безопасных покупок, позволяющую вернуть деньги.
- Если выбираете товар в российском интернет-магазине через «Яндекс. Маркет» почитайте отзывы о продавце.

Сбор персональных данных. Некоторые онлайн-магазины требуют указать на сайте не только номер телефона «для связи», но и еще множество другой информации, абсолютно не пригодной для целей покупки конкретного товара в конкретном магазине, например, знать отчество покупателя. Это похоже на какой-то попутный бизнес электронных продавцов – собрать побольше данных о своих покупателях, а затем продать их куда-то на сторону неизвестному спамеру или call-центру. Если заказываете товар с доставкой курьером, ограничьтесь указанием имени и номера мобильного телефона для связи. Если уж продавец настаивает на необходимости указать все Ваши данные, опишите себя вымышленными фамилией, именем, отчеством. Если заказать товар без указания дополнительной информации о себе невозможно, лучше выбрать другого продавца (попутно не лишним будет написать жалобу в Роскомнадзор о незаконном сборе персональных данных, благо сейчас это можно сделать, не выходя из дома).

Совет тринадцатый: по сохранению персональных данных.

- Заведите себе отдельную пластиковую карту для оплаты покупок через интернет, на которую переводите достаточную сумму непосредственно перед покупкой – так Вы сохраните остальные Ваши сбережения от пронырливых интернет-воришек.
- Стоит хорошенько запомнить, что сайты «приличных» электронных платежных систем всегда защищены сертификатами SSL. То есть если адрес сайта, через который Вы хотите провести оплату, начинается с «http://».

Банкинг или мобильный банк. Сегодня для перевода денег не обязательно идти в банк, стоять в очереди к операционисту, все можно сделать с помощью компьютера или мобильного телефона. В последние годы для удобства клиентов банки автоматически подключают при оформлении карты (или через некоторое время после оформления) такую услугу, как пополнение баланса мобильного телефона со счета карты. Причем для совершения такой операции необходим только сам телефон, к номеру которого привязана карта. Несомненно, новые сервисы по доступу к банковскому счету со смартфона очень удобны, но они таят в себе немалую опасность остаться без средств. К примеру, утрата телефона. Даже если у Вас не стоит мобильное приложение онлайн-банкинга, поставить его не составит особого труда. А смс-оповещения от Вашего банка будут приходить именно на этот телефон, находящийся в руках мошенника.

Совет четырнадцатый: как защитить смартфон от мошенников.

- Если у Вас к счету мобильного телефона привязана банковская карта, то в случае утраты мобильного телефона обязательно и срочно

блокируйте не только сим-карту, но и банковскую карту (в крайнем случае, позже ее можно будет разблокировать).

- Поставьте на Ваш смартфон антивирусное приложение.

Торренты и файлообменники. Принимая решение качать фильм или книгу через торрент-трекер надо помнить, что в Российской Федерации (а равно и в других цивилизованных странах мира) авторское право защищено законом. Это значит, что за незаконное размещение (а кое-где и за скачивание) фильма, книги, музыки и другой подобной информации с нарушением чужих авторских прав можно получить реальный штраф или даже срок заключения. Если сомневаетесь в «чистоте» авторских прав скачиваемого файла лучше поискать другие, легальные способы получить нужную информацию. Например, воспользоваться сайтом «онлайн-кинотеатр», где недорого, а может и бесплатно, но при наличии рекламы можно посмотреть приглянувшийся фильм. Неприятности могут ожидать при скачивании фильмов с незаконных сайтов: вирусы, спрятанные внутри архивов фильмов; кража денег с телефона**.** При попытке найти в интернете бесплатный контент в виде фильма или программного обеспечения пользователи периодически натыкаются на сайты, предлагающие ввести номер мобильного телефона. Выглядит это примерно так: «Напишите номер своего мобильного, Вам придет смс с кодом (или ссылкой), подтвердите ее получение ответной смс-кой (или нажмите на ссылку) и получите желанный фильм». Объясняется это защитой от «ботов», но на самом деле вполне возможно, что Вас подпишут на платную рассылку или спишут определенную сумму со счета телефона.

Совет пятнадцатый: как правильно пользоваться торрентами.

- Не вводите номер мобильного телефона на сомнительных сайтах.
- Не отправляйте ответных СМС и не активируйте пришедшие ссылки.

В консультации были представлены наиболее типичные угрозы при работе в сети Интернет и основные методы противодействия им. Будьте бдительны и внимательны сами и учите своих читателей основам безопасного Интернета.

Список полезных ссылок по интернет-безопасности

Азбука цифрового мира https://www.edu.yar.ru/azbuka/ Безопасность в сетевых сервисах, создание надежных паролей, работа с электронной почтой.

Виды мошенничества с персональными данными https://prolaw24.ru/criminal/moshennichestvo-s-pasportnymi-dannymi Что делать, если мошенники воспользовались персональными данными Вашего паспорта.

Безопасность в интернете https://www.tadviser.ru/index.php/ Безопасность в социальных сетях, киберзапугивание (кибербуллинг, кибersталкинг). Угрозы безопасности общения в мобильной сети.

Безопасность в соцсетях. Защитите свой аккаунт от мошенников http://security.mosmetod.ru/moshennichestvo-v-seti/92-bezopasnost-v-sotssetyakh Настройка приватности в соцсетях.

Безопасность в соцсетях https://vc.ru/social/81702-bezopasnost-v-socialnyh-setyah Правила безопасного общения в социальных сетях.

Безопасность в Интернете https://www.tadviser.ru/index.php/ Безопасность вебприложений, безопасность в соцсетях, информационная безопасность в банках и др.

Безопасность интернет-банкинга: основные средства защиты личного счета https://camafon.ru/internet/bezopasnost-platezhey О способах защиты счетов от мошенников.

Бессмертные спамеры: Почему «нигерийские письма» всё ещё работают https://secretmag.ru/trends/whatsup/ Фальшивые миллионеры и поддельные женихи расставили сети.

Блог «Человек и компьютер» http://itiman.ru/index.php/blog/60-moshennichestvo-v-internete О способах мошенничества в Интернете: фишинг, финансовые пирамиды, брачные аферисты и другое.

Ваши персональные данные: как их могут использовать мошенники?https://ichip.ru/tekhnologii/vashi-personalnye-dannye-kak-ikh-mogut-ispolzovat-moshenniki-410552 Советы о том, как защитить свои данные от чужого использования организациями и частными лицами.

Виды мошенничества в Интернете: схемы обмана и как с ними бороться https://sales-generator.ru/blog/vidy-moshennichestva-v-internete/
10 простых правил, как не попасться на уловки мошенников https://nyagan.life/advices/10-prostyh-pravil-kak-ne-popastsya-na-ulovki-moshennikov

Журнал Хакер – онлайн http://jurnali-online.ru/xaker Один из самых популярных журналов, посвященных информационной безопасности.

Закон о защите информации а интернете, технологии и средства https://scam.zone/stati/zaschita-informatsii-v-internete/ Нормативная база информационной безопасности. Что такое нигерийские письма, фишинг, фарминг и другие виды мошенничества.

Индефикация, аутенфикация и авторизация – в чем разница http://security.mosmetod.ru/moshennichestvo-v-seti/92-bezopasnost-v-sotssetyakh

Как защитить свой аккаунт на «Госуслугах», что такое PIN – код для смартфона, как подобрать себе пароль в течении одной минуты. Как безопасно загружать торрент-файлы https://ru.wizcase.com/blog/ Руководство для начинающих.

Как защитить себя от мошенничества в Интернете и что делать, если Вы уже потеряли свои деньги https://iklife.ru/udalennaya-rabota-i-frilans/moshennichestvo-v-internete-kak-obmanyvayut-moshenniki.html Разбор 19 схем обмана в Интернете.

Как не стать жертвой киберпреступника https://www.belta.by/infographica/view/kak-ne-stat-zhertvoj-kiberprestupnika-zaschita-bankovskoj-kartochki-16627/ Защита банковской карточки.

Как защитить персональные данные в сети Интернет https://mfc22.ru/news/50609/ Основные правила ответственного обращения со своей личной информацией в сети Интернет.

Компьютерра : легендарный журнал о современных технологиях https://www.computerra.ru/ Как безопасно скачивать торренты и не нарушать закон.

Лаборатория Касперского https://www.kaspersky.ru/ Информация о защите от вирусов, спама и хакерских атаках.

МедиаГвардия http://mediagvardia.ru/ федеральный проект, целью которого является объединение усилий интернет-пользователей для совместного выявления интернет-сайтов, сообществ и групп в социальных сетях, специализирующихся на распространении противоправного контента.

Мошенничество в интернете. Виды и способы защиты https://stop-obman.com/moshennichestvo-v-internete/ Фишинг, взлом аккаунтов в соцсетях, вирусы, покупки в Интернете.
Мошеничество в Сети http://security.mosmetod.ru/moshennichestvo-v-seti. Психология фишинга. Киберпреступники.

Онлайн – платежи http://security.mosmetod.ru/onlajn-platezhi Кража путем перехвата кодов в SMS. Взлом интернет – банкинга. Советы по защите денег и кредитных карт в интернете.

Твоя безопасность в соцсетях – ТОП 20 http://svagor.com/tvoya-bezopasnost-v-socsetyax-top-20 Принципы защиты личности в социальных сетях

Троллинг https://psihomed.com/trolling/ Что такое троллинг. Виды и причины троллинга.

Фонд «Разумный Интернет» https://xn--80akagffuicbyiyee4k.xn--p1ai/ Итоги цифрового диктанта для детей и взрослых: фишинговые сайты, безопасность при использовании банковской карты, какому интернет-магазину можно доверять и др.

Хейтеры кто это такие и что значит хейтить https://yandex.ru/turbo/vsvoemdome.ru/s/psihologiya/hejtery-kto-ehto На кого нападают хейтеры и как от них защититься.

Центр Безопасного Интернета в России https://www.saferunet.ru/ Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Интернет-угрозы и эффективное противодействием им в отношении пользователей.

Центр безопасности https://safety.google/families/ Краткие рекомендации помогут обеспечить безопасность членов семьи в Интернете.

Что мошенники могут сделать, зная ваши персональные данные https://www.sravni.ru/text/2020/7/23/chto-moshenniki-mogut-sdelat-znaja-vashi-personalnye-dannye/ Как защитить свои персональные данные от мошенников: наблюдения и советы.

Что такое нигерийские письма – мошенничество нигерийских спамеров https://www.stepandstep.ru/ Суть мошенничества нигерийских спамеров.