Безопасность в интернете

1 Общая безопасность в интернете.

В наши дни интернет стал неотъемлемой частью нашей жизни. С его помощью мы получаем информацию, общаемся, обмениваемся данными, оплачиваем товары и услуги, отправляем документы для поступления в вузы и делаем многое другое. Вместе с тем интернет таит в себе опасности — о них необходимо знать, чтобы избегать их.

В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Мошенники могут быть хорошо оснащены и использовать самые разные инструменты и методы — например, вирусное программное обеспечение (далее — вирусы), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и почтовых сервисах.

Вирусы.

Вирусы могут распространяться с помощью вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, на съемных носителях, через зараженные сайты. При этом сообщение с вирусом может быть получено как от постороннего человека, так и от знакомого, но уже зараженного участника социальной сети или почтовой переписки. Зараженными могут быть сайты, как специально созданные в целях мошенничества, так и обычные, но имеющие уязвимости информационной безопасности.

Рекомендации:

Использовать антивирусное программное обеспечение с обновленными базами вирусных сигнатур.
.
Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус.
.
Внимательно проверять доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).

Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.

Не подключать к своему компьютеру непроверенные съемные носители.

Не поддаваться на провокации злоумышленников, например, с требованием перевести деньги или отправить SMS, чтобы снять блокировку компьютера.

Мошеннические письма1.

1 Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги. В таких случаях они пишут письма определенного сценария. Один из примеров — так называемые «нигерийские письма», в которых автор обещает жертве огромную прибыль взамен на небольшие накладные расходы.

Пример «нигерийского письма»:

«Дорогой друг!

Я миссис Сесе-секо, вдова бывшего президента Заира (ныне Демократической республики Конго) Мобуту Сесе-секо. Я вынуждена написать Вам это письмо. Это в связи с моими нынешними обстоятельствами и ситуацией. Я спаслась вместе со своим мужем и двумя сыновьями Альфредом и Башером в Абиджан, Кот-д'Ивуар, где мы и поселились - затем мы переехали в Марокко, где мой муж умер от рака. У меня есть банковский счет на сумму 18 000 000 (восемнадцать миллионов) долларов США. Мне нужно ваше желание помочь нам - чтобы вы получили эти деньги для нас, в таком случае я представлю Вас моему сыну Альфреду, который имеет право получить эти деньги. Я хочу инвестировать эти деньги, но не хочу, чтобы было известно, что это делаю я. Мне хочется приобрести недвижимость и акции транснациональных компаний, а также вложиться в надежные и неспекулятивные дела, которые Вы посоветуете.

Искренне Ваша,

Миссис Мариам М. Сесе-секо»

Рекомендации:

Внимательно изучить информацию из письма. Проверить достоверность описанных фактов. Если в письме предлагается большая выгода за незначительное вознаграждение, скорее всего, оно мошенническое.

Игнорировать такие письма.

<u>Получение доступа к аккаунтам в социальных сетях и других сервисах.</u>

Злоумышленники часто стремятся получить доступ к аккаунтам жертвы, например, в социальных сетях, почтовых и других сервисах. Украденные аккаунты они используют, например, для распространения спам-писем и вирусов.

Мошенники могут получить доступ к учётной записи жертвы следующими способами:

Заставить жертву ввести свои данные на поддельном сайте.
Подобрать пароль жертвы, если он не вляется сложным.
Восстановить пароль жертвы с использованием "секретного вопроса" или введенного ящика электронной почты.

Перехватить пароль жертвы при передаче по незащищенным каналам связи.

Как правило, для кражи данных об аккаунтах используются фишинговые сайты. Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Злоумышленники создают фишинговые сайты, копирующие интерфейс известных ресурсов, а жертвы вводят на них свои логины и пароли, не понимая, что сайты поддельные.

Рекомендации:

Использовать сложные пароли (сложные пароли состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).

Никому не сообщать свой пароль.
Для восстановления пароля использовать привязанный к аккаунту мобильный номер, а не секретный вопрос или почтовый ящик.

Не передавать учетные данные — логины и пароли — по незащищенным каналам связи (незащищенными, как правило, являются открытые и общедоступные wi-fi сети).

Внимательно проверять доменные имена сайтов, на которых вводятся учетные данные.

2. Безопасность платежей в интернете.

В 2013 году ущерб от карточного мошенничества в России составил 4,6 млрд рублей (данные FICO), за год этот показатель вырос на треть. Это четвертое место по объему карточного мошенничества среди стран Европы (после Великобритании, Франции и Германии).

При этом большая часть мошеннических операций в интернете оказывается успешными по тем же причинам, что и в реальной жизни, – из-за таких людских качеств, как невнимательность, неосведомленность, наивность, беспечность.

В этом блоке мы постараемся выделить основные типы платежного мошенничества, с которыми сегодня сталкиваются пользователи Рунета, и постараемся дать основные рекомендации, как избежать обмана.

2.1 Распространенные примеры платежного мошенничества.

Фиктивные звонки от платежных сервисов

Мошенник может позвонить и представиться сотрудником банка или Яндекс.Денег 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.

Рекомендации:

- Помнить, что банки и платежные сервисы никогда не просят сообщать – ни по почте, ни по телефону – пароль, пин-код или код из SMS.
- Никому не сообщать пароли, пин-коды и коды из SMS от своего кошелька или банковской карты.

Выманивание SMS-пароля незнакомцем

Пользователю может прийти SMS от банка или платежного сервиса с паролем для совершения платежа. 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.

Рекомендации:

- Никому не сообщать пароли, пин-коды и коды из SMS, которые приходят на мобильный номер от банков, платежных сервисов, а также мобильных операторов.

Фальшивые письма от платежных сервисов

Пользователь может получить фальшивое письмо от имени Яндекс.Денег, своего банка или других платежных сервисов. Например, о том, что его счет заблокирован и для разблокировки необходимо перейти по ссылке и ввести свои данные.

Единственная цель таких писем — заставить пользователя перейти на поддельный (фишинговый) сайт и ввести там свои персональные данные, которые будут украдены. В дальнейшем эти данные могут быть использованы, например, для доступа к счету пользователя. Кроме того, на таком сайте компьютер может быть заражен вирусом.

Рекомендации:

- Помнить, что платежные сервисы и банки никогда не рассылают сообщения о блокировке счета по электронной почте.
- Не переходить по ссылкам из таких писем и не вводить свои пароли на посторонних сайтах, даже если они очень похожи на сайт банка, Яндекс.Денег или другого платежного сервиса.
- Перед вводом своих платежных данных на каких-либо сайтах проверять название сайта в браузере. Например, вместо money.yandex.ru фальшивый сайт может называться money.yanex.ru

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 в Яндекс.Деньгах. При этом, конечно же, никакого обещанного приза пользователь не получит.

Признаки фальшивой лотереи:

• Пользователь никогда не принимал участие в этой лотерее и вообще ничего о ней не знает;
• Пользователь никогда не оставлял своих личных данных на этом ресурсе или в этой организации, от имени которой приходит письмо;
• Сообщение составлено безграмотно, с орфографическими ошибками;
• Почтовый адрес отправителя – общедоступный почтовый сервис. Например, gmail.com, mail.ru, yandex.ru.

Фальшивые сайты авиабилетов

В интернете появилось множество сайтов, продающих поддельные авиабилеты. Цены на таких сайтах выгодно отличаются от других официальных онлайн-площадок для покупки билетов. Дизайн сайта при этом может выглядеть вполне аккуратно, а процесс платежа казаться привычным. На электронную почту даже придет подтверждающая бронь. Тем не менее покупка билета будет фиктивной, о чем пользователь может узнать только уже в аэропорту или позвонив в авиакомпанию.

Рекомендации:

- Перед покупкой услуги или товара на незнакомом сайте обязательно нужно проверять отзывы о нём в интернете. Если не удается найти положительные отзывы или нет вообще никаких пользовательских сообщений об этом ресурсе, это должно насторожить. Сайт может быть создан за один день, а закрыться уже на следующий или даже сразу после того, как на нем будет совершено несколько покупок.

Слишком выгодные покупки

Выгодную, но фальшивую покупку могут предложить пользователю где угодно – в интернет-магазине, в группе в соцсети, по электронной почте. На первый взгляд, объяснение может быть правдоподобное: подарили – не понравилось, это — распродажа конфискованного на границе товара и т.д. Оплатить такой товар предлагается онлайн — переведя деньги на банковскую карту, электронный кошелек или мобильный номер.

Рекомендации:

- Не доверять объявлениям о подозрительно дешевых товарах.
- Перед покупкой искать отзывы в интернете об интернет-магазине или частном продавце, который предлагает товар. Если информации нет или ее недостаточно, отказаться от покупки.

Фальшивые квитанции

Подделать могут не только сайт, но и бумажную квитанцию – например, за ЖКУ. (Также по поддельным квитанциям могут предлагать оплатить доставку книг, журналов и т.д. Для этих случаев действуют рекомендации из пункта «Слишком выгодные покупки».)

Рекомендации:

- Проверять реквизиты, указанные в платежке. Если они не совпадают с прежними, не оплачивать по счету. Информацию о смене реквизитов можно проверить по официальным телефонам (на квитанции они могут быть неверные).
- Проверять номер своего лицевого счета, указанный на платежке за ЖКУ. Он всегда один.
- Обратить внимание на дату получения платежки. Как правило, мошенники приносят поддельные квитанции раньше официальной даты оплаты, чтобы успеть собрать свои платежи.
- Настроить онлайн-платежи на заранее проверенные реквизиты и платить только по ним через проверенные сайты (сервис «Городские платежи», интернет-банк «Сбербанк.Онлайн», Альфа-Банк и др.)

Выпрашивание денег со взломанных аккаунтов в соцсетях или мессенджерах

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

Рекомендации:

- Всегда лучше перезвонить знакомому и уточнить, правда ли он сейчас нуждается в деньгах.
- Если возможности позвонить нет, можно задать какой-нибудь проверочный вопрос, ответ на который может знать только знакомый.

Фальшивые SMS якобы от знакомого

Мошенник может прислать SMS родителям пользователя с неизвестного номера, но якобы от имени пользователя. Например: «Мама, я попал в аварию, срочно нужны деньги, переведи их, пожалуйста, на этот номер телефона». «Папа, у меня проблемы, я в больнице, срочно нужны деньги, кинь их, пожалуйста, на этот кошелек. Маме не говори». Цель мошенника – выманить деньги у близких пользователя: они сами переведут их на указанный мобильный номер, электронный кошелёк или банковскую карту (в зависимости от того, какой способ будет указан в SMS).

Рекомендации:

- Связаться лично с пользователем, от имени которого прислано SMS,

чтобы проверить информацию. Например, позвонить ему.

Бесплатное скачивание файлов с подпиской

Часто, чтобы скачать бесплатный файл или посмотреть видео в хорошем качестве без рекламы, сайты предлагают ввести мобильный номер. Если сделать это, включится подписка и с указанного номера могут начать списываться деньги.

Рекомендации:

- Не указывать свой мобильный номер на незнакомых сайтах.
- Если подписка уже оформлена, позвонить в службу поддержки оператора и попросить отключить её.

2.2. Платежные данные, которые нельзя раскрывать.

Что делать? — если...

…вы потеряли карту.
Срочно позвоните в банк, попросите ее заблокировать и перевыпустить. Желательно, с новым номером. Пока вы не заблокируете карту, любой, у кого она окажется в руках, сможет воспользоваться ей — например, оплатить дорогую покупку в интернет-магазине.

…вам пришло уведомление о платеже, который вы не совершали.
Подайте в банк заявление о чарджбеке (отмене операции). В нём максимально подробно опишите произошедшее. Банк рассмотрит ваше обращение и вернет вам деньги. Не затягивайте с подачей заявления, чтобы обработка вашего чарджбека успела произойти в срок от 30 до 60 дней с момента совершения операции.
…вы забыли пароль от электронного кошелька.
Зайдите на сайт платежного сервиса и нажмите на ссылку "Восстановить пароль", система запросит мобильный номер, к которому привязан кошелёк. Укажите его, и на него придёт SMS с кодом для восстановления пароля.

2.3. Безопасность при оплате картами

Не сообщайте номер карты другим людям

Избежать проблем несложно, если придерживаться следующих рекомендаций:

Храните банковскую карту в надежном месте.

Не держите записанные пароли и коды рядом с картой.

Заведите отдельную карту для покупок в интернете.

Используйте для покупок в интернете только личный компьютер.

Регулярно обновляйте антивирусную защиту компьютера.

Старайтесь делать покупки в известных и проверенных интернет-магазинах.

Перед подтверждением оплаты убедитесь, что в адресе платежной страницы в браузере указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.

Подключите в банке услугу SMS-уведомлений, чтобы получать сведения о всех совершаемых платежах.

Сохраняйте отчеты об оплате и доставке товаров, которые вы получаете по электронной почте.

Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.

Использованы материалы https://www.apkpro.ru/content/blogcategory/34/113/