Яндекс

Материалы семинара «Безопасность в интернете»

18 октября 2014 года,
Москва

1. Общая безопасность в интернете

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.

Какие опасности могут поджидать в интернете

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

1.1. Вирусы

Вирусы могут распространяться с помощью вложенных файлов, ссылок в электронных письмах или в соцсетях, на съемных носителях, через зараженные сайты. Сообщение с вирусом может прислать как посторонний человек, так и знакомый, но уже зараженный участник социальной сети или почтовой переписки. Зараженными могут быть сайты, специально созданные в целях мошенничества, или обычные ресурсы, но имеющие уязвимости информационной безопасности.

Рекомендации

- Используйте антивирусное программное обеспечение с обновленными базами вирусных сигнатур.
- Не открывайте вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства связи, не удостоверившись, что файл или ссылка не содержит вирус.
- Внимательно проверяйте доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).
- Обращайте внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.
- Не подключайте к своему компьютеру непроверенные съемные носители.
- Не поддавайтесь на провокации злоумышленников, например, требование перевести деньги или отправить смс, чтобы снять блокировку компьютера.

1.2. Мошеннические письма

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 по определенному сценарию. Один из примеров — так называемые «нигерийские письма», в которых автор обещает жертве огромную прибыль в обмен на небольшую сумму.

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 изучите письмо. Проверьте достоверность описанных фактов. Если в письме предлагается большая выгода за незначительное вознаграждение, скорее всего, оно мошенническое.
- Игнорируйте такие письма.

1.3. Получение доступа к аккаунтам в социальных сетях и на других сервисах

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

Мошенники могут получить доступ к учетной записи жертвы следующими способами:

- Заставить жертву ввести свои данные на поддельном сайте.
- Подобрать пароль жертвы, если он не сложный.
- Восстановить пароль жертвы с помощью «секретного вопроса» или введенного ящика электронной почты.
- Перехватить пароль жертвы при передаче по незащищенным каналам связи.

Как правило, для кражи личных данных используются фишинговые сайты. Фишинг (от англ. **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

- Используйте сложные пароли (они 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 сообщайте свой пароль.
- Для восстановления пароля используйте привязанный к аккаунту мобильный номер, а не секретный вопрос или электронную почту.
- Не передавайте учетные данные — логины и пароли — по незащищенным каналам связи (не защищены, как правило, открытые и общедоступные wi-fi сети).
- Внимательно проверяйте доменные имена сайтов, на которых вводите учетные данные.

2. Безопасность платежей в интернете

Большая часть мошеннических операций в интернете оказываются успешными по тем же причинам, что и в реальной жизни, — из-за таких человеческих качеств, как невнимательность, неосведомленность, наивность, беспечность.

В этом блоке мы постараемся выделить основные типы платежного мошенничества, с которыми сталкиваются пользователи рунета, и дадим 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. Цель звонка — выманить платежные данные, с помощью которых можно украсть деньги с карты или из кошелька.

Рекомендации

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

Выманивание смс-пароля незнакомцем

Пользователю может прийти смс от банка или платежного сервиса с паролем для совершения платежа. Сразу после этого звонит человек, который говорит, что ввел этот номер мобильного телефона по ошибке, и просит сообщить код из смс, которое только что пришло пользователю. На самом деле код из смс — это пароль не к счету незнакомца, а к счету пользователя. С помощью пароля злоумышленник может поменять настройки кошелька или интернет-банка, украсть деньги и т.д.

Рекомендации

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

Фальшивые выигрыши в лотерее

Пользователь может получить сообщение (по телефону, почте или смс), что выиграл некий приз, а для его получения необходимо «уплатить налог», «оплатить доставку» или просто пополнить какой-то счет в Яндекс.Деньгах. Конечно, 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 ресурсе или в организации, от имени которой приходит сообщение.
- Сообщение составлено безграмотно, с орфографическими ошибками.
- Почтовый адрес отправителя — общедоступный почтовый сервис. Например, gmail.com, mail.ru, yandex.ru.

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 человека 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

- Помните, что платежные сервисы и банки никогда не рассылают сообщения о блокировке счета по электронной почте.
- Не переходите по ссылкам из таких писем и не вводите 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 проверяйте адрес сайта в браузере. Например, вместо money.yandex.ru фальшивый сайт может иметь адрес money.yanex.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 подтверждение брони. 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 нем в интернете. Если не удается найти положительные отзывы или какие-либо вообще, 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. Предложение может сопровождаться правдоподобным объяснением: подарили — не понравилось, распродажа конфискованного на границе товара и т.д. Оплатить покупку предлагается онлайн — переводом денег на банковскую карту, электронный кошелек или мобильный номер.

Рекомендации

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

Фальшивые квитанции

Подделать могут не только сайт, но и бумажную квитанцию — например, за ЖКУ. По поддельным квитанциям могут предлагать также оплатить доставку книг, журналов и т.д.

Рекомендации

- Проверяйте реквизиты, указанные в платежке. Если они не совпадают с прежними, не оплачивайте счет. Информацию о смене реквизитов можно проверить по официальным телефонам (на квитанции они могут быть неверные).
- Проверяйте номер своего лицевого счета, указанный на платежке за ЖКУ. Он всегда один и тот же.
- Обратите внимание на дату получения платежки. Как правило, мошенники предлагают поддельные квитанции раньше официальной даты оплаты, чтобы успеть собрать платежи.
- Настройте онлайн-платежи на заранее проверенные реквизиты и платите только по ним через проверенные сайты (сервис «Городские платежи», интернет-банк «Сбербанк.Онлайн», Альфа-Банк и др.)
- Используйте также рекомендации из пункта «Слишком выгодные покупки».

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 смс якобы от знакомого

Мошенник может прислать родственникам пользователя смс 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 кошелек или банковскую карту (в зависимости от того, какой способ будет указан в смс).

Рекомендации

- Свяжитесь с пользователем, от имени которого пришло сообщение, и проверьте информацию. Например, позвоните ему.

Бесплатное скачивание файлов

Часто пользователям, которые хотят бесплатно скачать файл или посмотреть видео в хорошем качестве без рекламы, предлагают ввести на сайте мобильный номер. Если так и сделать, может включиться платная смс-подписка и с указанного номера будут списываться деньги.

Рекомендации

- Не указывайте свой мобильный номер на незнакомых сайтах.
- Если подписка уже оформлена, позвоните в службу поддержки оператора мобильной связи и попросите 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 ею — например, оплатить дорогую покупку в интернет-магазине.

...вам пришло уведомление о платеже, который вы не совершали.

Подайте в банк заявление об отмене операции, где максимально подробно опишите произошедшее. Банк рассмотрит ваше обращение и вернет вам деньги. Не затягивайте с подачей заявления: оно должно быть обработано 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. Указав номер телефона, вы получите смс с кодом для восстановления пароля.

2.3. Безопасность при оплате картами

Обеспечить безопасность своей банковской карты несложно, если придерживаться следующих рекомендаций:

- Не сообщайте номер карты другим людям.
- 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 адресной строке браузера указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.
- Подключите в банке услугу смс-уведомлений, чтобы получать сведения о всех совершаемых платежах.
- Сохраняйте документы об оплате и доставке товаров, полученные по электронной почте.
- Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.

3. Рекомендации по подготовке уроков информационной безопасности

Чтобы выяснить, на какие виды мошенничества попадаются школьники, необходимо понять, для чего они используют интернет. Обычно это следующее:

- Поиск и получение информации
- Игры
- Общение (почтовые сервисы, социальные сети, средства передачи мгновенных сообщений)
- Просмотр мультимедиа (фильмы, музыка, изображения)
- Приобретение товаров и услуг

Мошенники могут получать прибыль таким образом:

- Использовать ресурсы устройства после его заражения вирусом
- Списывать средства с телефонного счета
- Выводить средства из электронного кошелька
- Списывать средства с банковской карты

Жертвами первых двух видов мошенничества могут стать даже первоклассники, так как многие из них уже имеют мобильные телефоны. Как только ребенок получает собственные электронные деньги (электронный кошелек или банковскую карту) или доступ к электронным деньгам взрослых родственников, на него начинают распространяться интернет-мошенничества, связанные со списанием средств.

Исходя из вышесказанного, предлагаем строить уроки по этой схеме:

Возраст	**Содержание урока**	**Дополнительные материалы**
Начальные классы	• Вирусные заражения с помощью электронных писем, сообщений и зараженных сайтов. • Получение доступа к учетным записям в социальных сетях, почтовых сервисах и т.д. • Смс-мошенничество.	Памятка родителям
Средние и старшие классы	• Вирусные заражения с помощью электронных писем, сообщений и зараженных сайтов. • Получение доступа к учетным записям в социальных сетях, почтовых сервисах и т.д. • Смс-мошенничество. • Безопасность платежей в интернете.	Памятка родителям

Если у вас появятся вопросы, напишите нам:

- sterh@yandex-team.ru (для вопросов о мошенничестве в интернете);
- pr@yamoney.ru (для вопросов о безопасности платежей);
- ege-support@yandex-team.ru (для вопросов о тестах на Яндекс.ЕГЭ).