БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Автор:
Сарбаева Любовь Владимировна,
учитель информатики и ИКТ,
ГБОУ СОШ №10

г.о. Чапаевск, 2014г.

27 октября 2014 г. состоялась конференция Российской Ассоциации Электронных Коммуникаций (РАЭК) *«GENERATION NEXT. ДЕТИ 2014»,*

посвященная проблематике защиты детей в информационном пространстве.

Информация по адресу:

http://runet-id.com/event/next2014/

Использование Интернета в образовательной деятельности связано со многими позитивными факторами.

Вместе с тем, существуют риски негативного влияния сети Интернет на здоровье пользователя.

«Что вы знаете об угрозах, которые исходят из Интернета?»

С целью защиты детей и подростков от вредоносной информации Роскомнадзором совместно с экспертным сообществом ведущих российских педагогов и ученых

разработана Концепция информационной безопасности детей

(http://rkn.gov.ru/mass-communications/p700/p701),

которая в настоящее время прошла общественное обсуждение.

Безопасность в интернете

1. Общая безопасность в интернете

1.1 Вирусы

Вирусы могут распространяться с помощью вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, на съемных носителях, через зараженные сайты.

Рекомендации:

- Использовать антивирусное ПО 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.

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 определенного сценария.

Один из примеров — так называемые «нигерийские письма», в которых автор обещает жертве огромную прибыль взамен на небольшие накладные расходы. Пример «нигерийского письма»:

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»***

1.3 Получение доступа к аккаунтам в социальных сетях и других сервисах

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

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

2.1 Распространенные примеры платежного мошенничества. Основные рекомендации, как избежать обмана

1) Фиктивные звонки от платежных сервисов

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.

2) Выманивание SMS-пароля незнакомцем

Рекомендации: -

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

3) 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.

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 Денеги 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

4) Фальшивые выигрыши в лотереи

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**

5) 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.

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***

6) Слишком выгодные покупки

Выгодную, но фальшивую покупку могут предложить пользователю где угодно – в интернет-магазине, в группе в соцсети, по электронной почте. 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**

7) 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.)

8) Выпрашивание денег со взломанных аккаунтов в соцсетях

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.**

9) 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».*

<u>Цель мошенника</u> – выманить деньги у близких пользователя:

Рекомендации:

- **Связаться лично с пользователем, от имени которого прислано SMS, чтобы проверить информацию. *Например,* позвонить ему.**

10) 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. В нём максимально подробно опишите произошедшее. Не затягивайте с подачей заявления, чтобы его обработка 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.**

На сайте «Дети онлайн» www.detionline.com открыта *линия телефонного и онлайн-консультирования,* которая оказывает психологическую и информационную поддержку детям и подросткам, столкнувшимся с различными проблемами в Интернете.

Целевая аудитория — дети, подростки, родители и работники образовательных и воспитательных учреждений.

Служба Линия помощи «Дети Онлайн» включена в базу единого федерального номера телефона доверия для детей, подростков и их родителей.

на Линию помощи можно позвонить по телефону 8-800-25-000-15, бесплатно из любой точки страны, либо по электронной почте: helpline@detionline.com. Звонки принимаются в рабочие дни с 9.00 до 18.00 по московскому времени

Дать ответ на вопрос:

«Для чего нужно знать основные правила безопасной работы в Интернете?».

Спасибо за внимание!!!