Тема: Интернет-мошенничество и способы его предупреждения.

Составитель – педагог дополнительного образования Франчук С. Г

слайд 2

Цель: познакомить родителей с различными видами Интернет–мошенничества и способами их предупреждения.

Оборудование: компьютер, проектор, мультимедийная презентация.

Прежде чем начать обзор видов интернет-мошенничества, давайте выясним, какие действия попадают под разряд мошеннических.

слайд 3

Согласно определению свободной энциклопедии «Википедия»:

"***Мошенничество*** *– это хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Форма мошеннических обманов очень разнообразна. Обман может совершаться в виде устного или письменного сообщения, либо заключаться в совершении каких-либо действий.*

Мошенники действуют почти в каждой сфере человеческой деятельности - естественно, не могли они обойти своим вниманием и интернет.

Что такое мошенничество в Интернете? Термин «мошенничество в Интернете» применим в целом к мошенническим махинациям любого вида, где используются один или несколько элементов Интернета – такие как комнаты в чатах, электронная почта, доски объявлений или веб-сайты – для привлечения потенциальных жертв, проведения мошеннических сделок или для передачи поступлений от мошенничества в финансовые учреждения или иным лицам, участвующим в таких махинациях.

слайд 4

Очень часто старшие школьники имеют в своем распоряжении определенные суммы денег.Это деньги, которые дают родители на карманные расходы, подаренные родственниками, заработанные во время каникул. И этими деньгами ребенок уже может распоряжаться самостоятельно. Но его нужно научить, как и для чего правильно потратить ту или иную сумму и предупредить, об опасностях подстерегающих неопытного покупателя, если денежные операции совершаются в сети Интернет.

Предлагаю вам рассмотреть самые распространенные виды мошенничества в Интернете.

слайд 5

1.Недобросоветные Интернет-магазины.

Многие, наверное, согласятся, что совершать покупки по Интернету –это удобно, быстро, просто. Для того, чтобы радость онлайн-покупок не была омрачена получением некачественного товара или потерей денег рекомендуем обратить внимание на некоторые признаки потенциально опасных Интернет-магазинов:

- низкая цена. Мошенники часто используют данный прием для привлечения клиентов.

- требование предоплаты. Продавец предлагает перечислить предоплату за товар, особенно с использованием анонимных платежных систем, электронных денег или при помощи банковского перевода на карту, выданную на имя частного лица.

- отсутствие возможности курьерской доставки и самовывоза товара. Покупатели вынуждены пользоваться для доставки товара услугами транспортных компаний и, соответственно, вносить предоплату.

- отсутствие контактной информации и сведений о продавце. На сайте Интернет-магазина отсутствуют сведения об организации или индивидуальном предпринимателе, а контактные сведения представлены лишь формой обратной связи и мобильным телефоном.

- отсутствие у продавца или магазина «истории». Если Интернет-магазин или учетная запись продавца зарегистрированы несколько дней назад, сделка с ними может быть опасной.

- неточности или несоответствия в описании товаров.В описании товара присутствуют явные несоответствия или ошибки.

- излишняя настойчивость продавцов и менеджеров.

В процессе совершения покупки менеджер магазина начинает торопить вас с заказом и оплатой товара, убеждая в том, что если не заказать его сейчас, то цена изменится или товар будет снят с продажи.

Из всего вышесказанного можно сделать вывод, что если Интернет-магазин соответствуют хотя бы одному из указанных признаков, это серьезный повод задуматься о целесообразности совершения сделки. Если под их описание подходят два или более признака, рекомендуется воздержаться от контактов с данным продавцом или магазином. Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности и, если Ваш ребенок уже совершает онлайн-покупки самостоятельно, объясните ему простые правила безопасности.

слайд 6

Перед совершением покупки необходимо:

1.Ознакомиться с отзывами покупателей.

2. Проверить реквизиты и название юридического лица – владельца магазина.

3. Уточнить, как долго существует магазин.

4. Узнать, выдает ли магазин кассовый чек.

5. Сравнить цены в разных интернет-магазинах.

6. Позвонить в справочную магазина.

7. Обратить внимание на правила интернет-магазина.

8. Выяснить, сколько точно придется заплатить за заказ.

слайд 7

2.Предложения по составлению гороскопа.

Объявления, предлагающие заказать персональный гороскоп, очень часто можно увидеть во Всемирной паутине. Авторы обещают выслать его быстро и бесплатно. Пользователю предлагается заполнить стандартную анкету (имя, фамилия, дата рождения) и, конечно, оставить свой электронный адрес. Любитель астрологии указывает все эти данные, но вместо гороскопа в его ящик попадает письмо с еще одним условием: чтобы получить заказ, надо отправить по указанному номеру SMS-сообщение с набором тех или иных цифр. Если клиент производит платеж, то со счета его мобильного списывается сумма в несколько сотен рублей. В лучшем случае ему действительно пришлют гороскоп. Причем сразу же, что уже вызывает сомнения в его уникальности. В худшем — не пришлют ничего.

слайд 8

3.Акции “Помогите ребенку!”

Это самый кощунственный вид интернет-мошенничества, поскольку речь идет о спекуляции на больных детях. Текст о тяжелобольном ребенке с его фото рассылается по почтовым ящикам или вешается на интернет-форум. Автор послания рассказывает слезную историю о мальчике (девочке), чьи родители не могут оплатить дорогую операцию или покупку лекарств. Всем, кто хочет помочь, предлагается перечислить деньги на банковский счет (реквизиты прилагаются) или произвести оплату через систему “Веб-мани”.

Авторы таких посланий могут повесить в Интернете как фото реально больного малыша, взятое с благотворительного сайта, так и любое чужое. Благодаря чему дошло до того, что граждане, обнаружив в Интернете

любую просьбу о помощи, перестают верить таким объявлениям и порой отворачиваются от людей, действительно нуждающихся в срочном лечении.

Совет: увидев объявление о сборе денег для ребенка и желая помочь ему, установите с его автором или родственниками больного личный контакт. Уточните фамилию ребенка, диагноз, в какой больнице лежит. И договоритесь о передаче денег из рук в руки.

слайд 9

4.Предложения надомной работы.

Искусством наживаться на тех, кто ищет работу, российские мошенники овладели еще в доинтернетовские времена. Просто перенесли свою простую схему во Всемирную паутину.

Аферисты вешают в Сети объявления о том, что им требуются наборщики текстов. Желая подработать, люди отвечают на такие предложения. Заполнив высланные анкеты и получив положительный ответ лже-издательства просят за пробный заказ перевести им в качестве залога за рукописные страницы по системе “Яндекс.Деньги” или “Веб-мани” 50-100 рублей. Это будет гарантией того, что вы выполняете заказ. Естественно, после перевода денег, все связи с такими работодателями прекращаются.

слайд 10

5.“Мобильник в подарок!”

Сейчас наиболее популярны два способа таких афер.

Первый используют недобросовестные интернет-магазины. Они объявляют на своих сайтах, что начинается розыгрыш дорогого мобильного телефона. Для участия необходимо,например, купить у них два диска (музыкальных или игровых), а в конце недели якобы будет происходить розыгрыш среди покупателей. Но увидеть того, кто выиграл, вам, понятно, никто не даст. Хотя на сайте магазина через пару дней и появится информация, что количество выигравших на этой неделе увеличилось.

Второй способ еще проще: мошенники устраивают что-то типа аукциона. Они предлагают вам отправлять на определенный номер SMS. Естественно, платные. Кто больше пришлет, тому дорогой телефон и достанется. Подогревать ваш азарт будут приходящие на почтовый ящик сообщения о том, что вы отстаете от лидера всего на пару-тройку SMS. В итоге вы истратите все деньги на сотовом, а вам сообщат: “Вы прислали 25 сообщений, а выигравший — 26. Попробуйте в следующий раз”.

НО! Не все вышеперечисленные интернет-объявления являются мошенническими. Но стоит ли рисковать? Лишиться 500—1000рублей — это, может для кого то и не накладно. Однако для мошенника получить по 500рублей от двадцати азартных людей, — хорошая прибыль.

слайд 11

6. Неполная или искаженная поставка компьютерного ПО, с помощью которого похитители выкрадывают средства пользователей. Заказывая и оплачивая в сети интернет у непроверенных поставщиков ПО, вы рискуете, заплатив деньги, получить не весь комплект ПО, нерабочие программы, либо программы зараженные вирусами. Очень часто предлагаю скачать бесплатно игру или программу, но для того чтобы распаковать скачанный архив, нужно отправить СМС-сообщение на указанный номер. Стоимость такого СМС-сообщения может варьировать от 50 до 1000 рублей.

Совет: приобретайте лицензионное программное обеспечение у проверенных поставщиков.

Сегодня мы попытались собрать воедино самые популярные на сегодняшний день виды кибермошенничеств и предупредить о них вас.
Каждому кажется: обмануть или ограбить могут кого угодно, но только не меня. Особенно если это касается махинаций в Интернете. Даже те, кто однажды попал на удочку аферистов, уверены: теперь я осторожен и больше этого не произойдет. Но дело в том, что Всемирная паутина — бездонная бочка всяческих афер. Ее открытость, а главное, юридическая безнаказанность, способствуют созданию все новых и новых ухищрений. Гражданам остается лишь набивать шишки и делиться печальным опытом со знакомыми.

слайд 12

Самыми незащищенными участником интернет-сообществаявляется дети, именно они чаще всего становятся потенциальными жертвами мошенников. И только вы, родители, можете уберечь своих детей от совершения необдуманных действий, построив с ребенком такие доверительные взаимоотношения, когда всеми своими сомнениями он будет делиться именно с вами,и совет просить именно у вас, а не у виртуальных собеседников в сети.

слайд 13

Спасибо за внимание!

Использованные ресурсы:

1. http://aferizm.ru/novost/2014/11/141124-1-internet-shop.htm«О признаках мошенничества при выборе Интернет-магазина»
2. https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D1%82%D0%B2%D0%BE «Википедия»
3. http://antifraud.renovu.ru/ «Проект «Ренову́»