МУНИЦИПАЛЬНОЕ КАЗЕННОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 12»

Исследовательская работа

«МОШЕННИЧЕСТВО В СЕТИ ИНТЕРНЕТ»

Автор:

Нагаева Анжелика Юрьевна,

учитель информатики

х.Графский

2023 г.

Содержание

Введение

Мошенничество в Интернете — это большая проблема для современного мира. Дело в том, что одновременно с прогрессом, на два шага вперед развиваются способы обмана обычных пользователей. Это достаточно обширная проблема, ведь Интернет – это огромная паутина захватившая весь мир. И в ней можно оставаться анонимным, поэтому процент раскрытия преступлений очень невелик. Однако благодаря хорошему информированию о новых способах мошенничества, становиться все меньше и меньше жертв.

Актуальность:

В современном мире мы все больше проводим времени в Интернете, там большая часть нашей работы, вся информация и связь с людьми, нам стало привычно находить всю информацию в сети. Мы совершаем покупки по Интернету и это стало совсем обычным делом. Но одновременно с этим развивается и мошенничество в Интернете. Поэтому я считаю, что эта проблема достаточно актуальна в наши дни.

Проблема:

Какие правила нужно соблюдать, чтобы не попасться на уловки мошенников в Интернете?

Гипотеза исследования - избежать обмана в сети Интернет возможно в случае хорошей информированности пользователей сети Интернет.

Объект исследования: всемирная сеть Интернет.

Предмет исследования - мошенничество в сети Интернет.

Цель исследовательской работы - выявить основные виды мошенничества

Интернете; разработать рекомендации безопасного пользования ресурсами сети Интернет.

Задачи исследования:

- изучить основные виды мошенничества в сети Интернет;

- провести анкетирование

- дать общие рекомендации по защите от мошенничества в сети Интернет.

Практическая значимость

Если гипотеза подтверждается, следовательно, можно утверждать, что избежать обмана в сети Интернет возможно в случае хорошей информированности пользователей сети Интернет. В работе использованы такие методы исследования как исследование и обобщение.

Глава 1. Интернет мошенничество

1.1 История появления мошенничества

Интернет-мошенничество появилось во времена, когда интернет стал массово входить в каждый дом. В 90-х годах прошлого столетия, с появлением доступа к персональным компьютерам и внедрения Интернета в широкие массы населения, появилась не только положительная сторона в быстром получении информации, но и угроза, вызванная действиями интернет-мошенниками. Как правило в этот период мошенники завоевывали незаконным путем личные данные пользователей Интернет:

-логины и пароли для подключения к сети Интернет по средствам Dial-up (телефонные линии), для его использования за счет своих жертв;

-логины и пароли от почтовых ящиков, для хищения информации из электронных писем.

В 2000-е годы с массовым внедрением банковских карт и способностью их онлайн оплаты, появилось экономическое мошенничество, ее целью является хищение информации о банковской карте (номер карты, срок действия, фамилии и имени держателя, а также секретного кода CVC) жертвы, для осуществления платежа или перевода денежных средств в карман мошеннику.

С появлением интернет-магазинов, а также различных площадок с объявлениями в Интернете, мошенники так же нашли способ обманывать своих жертв продавая отличный от описания, либо несоответствующего качество, в других случаях и вовсе несуществующий товар.

Массовая регистрация и пользование социальными сетями, так же нашло применение для корыстных целей мошенников. Злоумышленники стали пользоваться чувствами людей, такими как жалость и доверчивость. В социальных сетях публикуются объявления о помощи больным детям и письма с просьбой о помощи от родственников, знакомых, вместо которых сидит мошенник и просит деньги в виде перевода на карту или иную банковскую систему.

1.2 Влияние мошенничества на пользователей Интернета

Типы людей подверженных к действиям мошенников.

Как правило, на уловки мошенников попадаются пользователи, которые не осведомлены о безопасности пользования Интернетом и являются доверчивыми, и не разбираются в принципах информационной безопасности.

Люди, относящиеся к таким типам, очень легко идут на контакт с мошенниками и без колебаний передают всю необходимую от них информацию, не подозревая об угрозе и последствиях. Отношение к информационному пространству Интернет пользователей после действий мошенников Жертвы мошеннических действий, а также пользователи, знания которых недостаточны для защиты своих личных данных, зачастую перестают пользоваться и доверять ресурсам, находящимся в сети:

- интернет-магазинам,
- площадкам с объявлениями,
- личным кабинетам банковских услуг и т.п.

Помимо этого, вселяя страх на пользование этих ресурсов своим знакомым и друзьям делясь горьким опытом

1.3 Основные виды интернет-мошенничества

Интернет-попрошайничество

С того времени как в мире появился интернет - в сети сразу появилось попрошайничество. Хитрые дельцы стали выманивать у других пользователей деньги под различными предлогами: на благотворительность, сборы на пожертвования, да и просто выпрашиванием денег. Существуют профессиональные нищие, которые выманивают деньги на улице и за счет этого живут. Аналогичные мошенники прекрасно себя чувствуют и в интернете. Зачастую на сайте помещается баннер, на котором изображены дети или инвалиды, якобы тяжело больные. Вас просят перевести деньги на номер кошелька, либо на карту банка. Большинство из подобных просьб носят мошеннический характер. Мошенники работают очень профессионально, они мастерски обманывают и пишут жалостливые тексты, настоящие крики о помощи. Особо хитрые - создают профессиональные сайты мифических фондов помощи и просят деньги там. А баннеры своего "фонда" - вешают на других сайтах, сердобольные пользователи переходят по ним и отправляют жуликам свои кровные деньги. Такие "фонды" - могут зарабатывать достаточно крупные деньги на порядочных гражданах. В последнее время также стали популярными просьбы о помощи православному храму или священнику - мы рекомендуем тщательно проверять тех, кому вы переводите деньги. Лучше всего отнести деньги в храм самим. Как не стать жертвой мошенников? Рекомендуем делать пожертвования только в известные вам фонды, обычно в попечительском совете подобных фондов есть известные люди - актеры, музыканты, звезды шоу бизнеса и т. д.

Фальшивые антивирусы

Киберпреступники постоянно ищут новые способы манипуляции своими жертвами в Интернете. А один из самых значительных барьеров на пути кибератаки — это осведомленность и бдительность. Именно поэтому стоит знать о фальшивых антивирусах. Они обычно очень похожи на настоящие, только не защищают от вирусов. А еще приносят много других проблем. Чаще всего они попадаются на сомнительных сайтах, поэтому стоит быть вдвойне внимательным, нажимая какую-либо ссылку. Однако если поддельные антивирусы настолько правдоподобно выглядят, то как же от них защититься?

Никогда не устанавливайте никакие программы, не проведя поиск в Интернете по их названию. Реклама самой фирмы обычно не самый надежный источник информации об интересующей программе. Слепо нажав на какую-то ссылку в рекламном баннере или письме, вы запросто можете попасть на вредоносный сайт, с которого на ваш компьютер загрузится нечто неприятное, о чем вы даже не узнаете сразу. Чем больше вы об этом знаете, тем в большей безопасности находитесь. Поэтому не стесняйтесь перед установкой программы выполнить быстрый поиск по интересующему вас антивируснику с целью найти больше информации.

Взломы аккаунтов

Сегодня почти у каждого пользователя сети интернет есть свой аккаунт в популярных социальных сетях таких как фейсбук, Контакте и т.д. Мошенники могут взломать вашу страничку в социальной сети и потребовать послать смс на платный короткий номер при Вашей попытке входа в аккаунт. Ни в коем случае не стоит этого делать. За смс с Вас снимут не менее 300 рублей, а для разблокировки вашего аккаунта достаточно указать Ваш номер мобильного и Вам на него придет смс с Вашим новым паролем. Эта операция совершенно бесплатна. Если Вы в чем-нибудь сомневаетесь, сразу обращайтесь в службу поддержки.

Электронные кошельки

На сегодняшний день все больше людей заводят себе электронные кошельки. Это удобные и безопасные средства расчётов в сети интернет. Самые популярные из них: Яндекс Деньги, Qiwi кошелёк и т.д. Мошенники активно используют e-mail рассылку от имени тех. поддержки той или иной платёжной системы. Обычно в письме говорится, что Ваш интернет кошелёк заблокирован (или может быть заблокирован, или требуется его повторная активация и т.п.) и Вам необходимо пройти по ссылке ниже, где ввести свои личные данные (логин, пароль). Причём и e-mail адрес отправителя данного письма может соответствовать адресу Вашей тех. поддержки, и страница, на которую Вы попадаете, перейдя по ссылке из письма, будет такой как на официальном сайте. Нужно чётко понимать, что официальная тех. поддержка никогда не будет спрашивать у Вас идентификационные данные (логин, пароль). Если Вам пришло такое письмо, я рекомендую зайти на официальный сайт компании Вашей платёжной системы и написать письмо в службу безопасности, подробно описав проблему.

Фишинг

Фишинг (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам. Избежать угона очень просто, достаточно знать, что сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее. Если же у вас всё-таки украли аккаунт, вернуть его, как правило очень просто, достаточно обратиться к технической поддержке сайта и доказать, что этот аккаунт – ваш. Обычно с вас потребуют ответить с почтового ящика, если вы переводили деньги на этот аккаунт, показать фотографии квитанции перевода, или получить подтверждение с помощью sms, если вы привязали аккаунт к телефону.

Нигерийские письма

«Нигерийские письма» — распространённый вид мошенничества, получивший наибольшее развитие с появлением массовых рассылок по электронной почте (спама). Письма названы так потому, что особое распространение этот вид мошенничества получил в Нигерии, причём ещё до распространения Интернета, когда такие письма распространялись по обычной почте. Однако нигерийские письма приходят и из других африканских стран, а также из городов с большой нигерийской диаспорой (Лондон, Амстердам, Мадрид, Дубай). Рассылка писем началась в середине 1980-х гг. Как правило, мошенники просят у получателя письма помощи во многомиллионных денежных операциях, обещая солидные проценты с сумм. Если получатель согласится участвовать, у него постепенно выманиваются все более крупные суммы денег якобы на оформление сделок, уплату сборов, взятки чиновникам, и т. п. Достаточно не доверять кому попало. Если же вы все-таки повелись на такой глупый обман, то вам, как правило, ничего не поможет, вся ответственность за распределение денег лежит на вас. Это не все виды мошенничества, но большинство из них очень похожи друг на друга, все они основаны на доверии пользователя, часть из них работают с помощью вредоносных программ.

Кардинг

Кардинг - вид мошенничества связанный с банковскими картами. Мошенники активно пытаются получить ваши данные по карте и сразу по ним что-нибудь купить или обналичить. Реализуется самыми разными способами, в том числе фишингом, фармингом и, просто создавая интернет-магазины, которые на самом деле ничего не продают, а просто собирают данные по картам.

Программы – пустышки, обманщики, фейки.

Все сталкивались с платными программами - архивами, которые чтобы распаковать файл требуют отправить смс. В 99,9% случаев это обман. Почему? Вы скачиваете архив себе на компьютер, распаковываете его, и в этот момент появляется окошко такого вида: «Введите номер своего мобильного телефона, и мы пришлем вам код активации программы». Вы вписываете свой номер, получаете код, после чего недосчитываетесь на своем лицевом счету крупную сумму денег. Это тоже своего рода мошенничество, правда, куда более «официальное» (что-либо доказать достаточно трудно). Ну а что касается программы, то она, как правило, представляет, из себя обыкновенную «пустышку», которая ничего не умеет делать. Все? Как бы, не так! Дело в том, что с вашего лицевого счета была списана отнюдь немаленькая сумма! Более того, она может продолжать списываться через определенное время. Это так называемая подписка, от которой нужно отписаться. Для этого надо отправить слово STOP или СТОП на четырехзначный номер, который вы можете узнать у своего оператора связи. Что в итоге мы имеем? А то, что, находясь в Интернете, надо быть, как можно более аккуратным, иначе можно лишиться денежных средств.

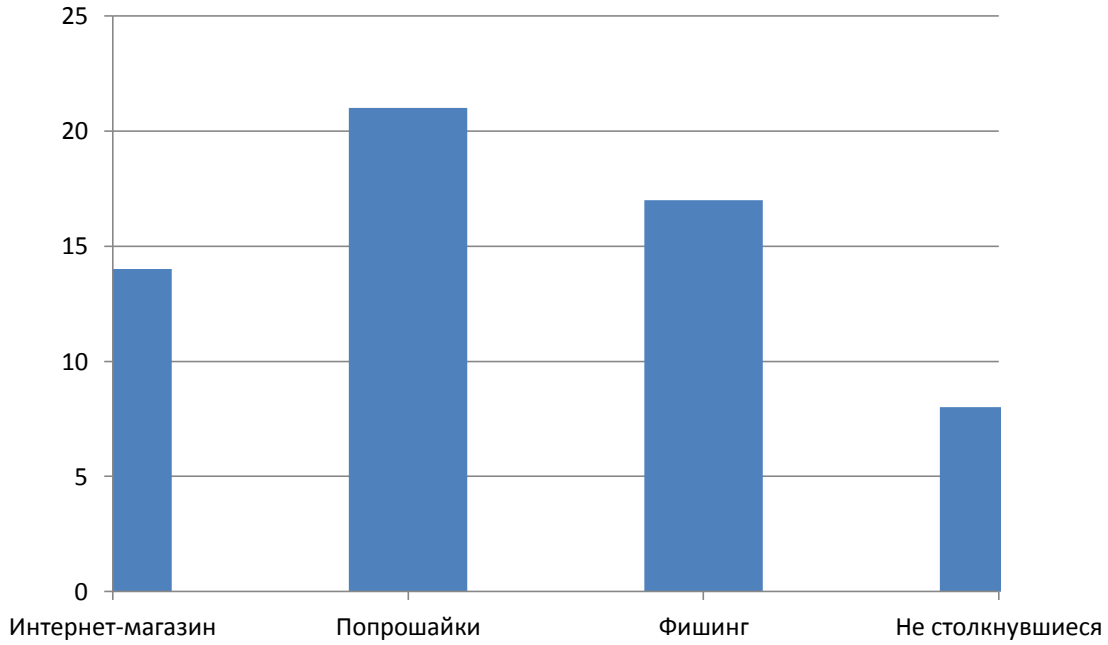
Будьте внимательны!

Глава 2. Информационная безопасность в сети интернет

Информационная безопасность- это система мер, направленная на предотвращение несанкционированного доступа, раскрытия, использования или уничтожении информации.

2.1 Исследование уровня информационной безопасности

Мной был проведен опрос в социальной сети ВКонтакте. Всего было опрошено: 60 человек. Всем респондентам был задан один вопрос: с какими видами мошенничества Вы сталкивались в Интернете? Результаты опроса таковы:



По результату опроса лиши 1/3 респондентов хоть раз в жизни сталкивались с виртуальными мошенниками – это 33%. Наиболее распространенным видом мошенничества по опросу является размещение объявления с просьбами помочь больному ребенку или сироте – 40%, затем фишинг – 35% и интернет-магазины – 30%.

Как не стать жертвой мошенников

Основными признаками мошенничества являются:

- навязчивая реклама, обещающая огромный доход без вложения знаний и большого труда;
- требование ввода ваших персональных данных на сомнительных ресурсах;
- требование отправки смс;
- заманчивые предложения, приходящие через почту от незнакомых людей.

Как правило, это спам разосланный многим с цель на ком-нибудь поживиться.

2.2 Рекомендации по безопасному использованию ресурсов сети Интернет:

Не дайте себя обмануть!

- ✓ Не отправляйте СМС на короткие номера, не узнав прежде их реальную стоимость.
- ✓ Не оставляйте номер своего мобильного на сомнительных сайтах!
- ✓ Всегда проверяйте контактные данные, представленные на сайте компании или частного лица, с которыми планируете иметь дело.
- ✓ Проверьте регистрационные данные самого сайта, на какую компанию или частное лицо было зарегистрировано доменное имя и как давно.
- ✓ Если Вам предлагают работу, то платить должны Вам, а не Вы.
- ✓ Не отправляйте деньги за регистрацию, за почтовые расходы, как залог комплектующие, с которыми Вам предстоит работать и т. п.
- ✓ Почитайте отзывы других пользователей сети об этой компании, сайте или частном лице.
- ✓ Не открывайте файлы, которые прислали неизвестные Вам люди. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
- ✓ Не добавляйте незнакомых людей в свой контакт (ICQ, MSN messenger и т.д.)
- ✓ Ни под каким предлогом не выдавай незнакомым людям свои личные данные (домашний адрес, номер телефона и т.д.) и пароли.
- ✓ Старайся не нажимать на рекламные баннеры, даже если они кажутся тебе очень заманчивыми.
- ✓ Не оставлять своих персональных данных на открытых ресурсах.
- ✓ Не проходи по ссылкам в спамовых письмах.

Заключение

Мошенничество, увы, неискоренимо. И на просторах Интернета оно подстерегает нас везде: в электронной почте, социальных сетях, на различных сайтах. С годами злоумышленники изобретают новые приемы, но основные механизмы обмана не меняются. Только сам пользователь может сделать свою жизнь в виртуальном пространстве безопасной. Я надеюсь, что предоставленная информация будет вам полезна.

В исследовательской работе я представила лишь мизерную долю того многообразия видов мошенничества, что есть в Интернете. Если описывать все варианты, то получится целая книга из нескольких томов! У меня была цель не только перечислить и описать способы отъема денег при помощи Интернета, а донести до вас, что никто просто так в Интернете денег не дает. Не стоит верить в обещания об огромных заработках уже через неделю, реальная работа в Интернете – это действительно работа в полном смысле этого слова. Есть много честных способов заработка при помощи Интернета, они требуют усилий и времени.

Изучив результаты анкетирования, я пришла к выводам, что не каждый знает об опасностях, подстерегающих их на просторах сети Интернет. Моей задачей являлось выявить и устранить этот пробел в знаниях людей. На мой взгляд, я с ней справилась.

Цель исследовательской работы по информатике «Мошенничество в сети Интернет» достигнута. Продукт нашей деятельности позволяет ознакомится с основными правилами безопасного использования сети Интернет. Позволяет рассказать об этом родственникам и друзьям, что уменьшит риск быть обманутым в Интернете.

Не стоит думать, что Интернет – это безопасное место, в котором можно чувствовать себя полностью защищенным. Чтобы максимально обезопасить себя и своих близких от опасностей сети Интернет, нужно постоянно совершенствовать свои знания и навыки в области информационной безопасности в сети Интернет.

Список литературы

1. Баранов, И.Р. Виды телекоммуникационного мошенничества / И.Р. Баранов // Вестник Владимирского юридического института. – 2015. – № – С. 218-243.
2. История развития мошенничества, современные виды мошенничества и способы борьбы с ними - Алпатов, А.С. Мошенничество и причинение имущественного ущерба путем обмана или злоупотребления доверием / А.С. Алпатов // Трибуна молодого ученого. – 2016. – № 2. – С. 16-37.
3. Колескин Д. В. История развития мошенничества, современные виды мошенничества и способы борьбы с ними // Социально-гуманитарные проблемы современности: сборник научных трудов по материалам Международной научно-практической конференции 24 апреля 2020г. : Белгород : ООО Агентство перспективных научных исследований (АПНИ), 2020. С. 37-42.

Перечень информационных ресурсов

• Бизнес статьи Каким бывает мошенничество в интернете?

https://businessman.ru/new-kakim-byvaet%20moshennichestvo_v_internete.html

• Способы обмана в глобальной сети

http://consumersjournal.org/moshennichestvo/sposoby-obmana-v-globalnoj-seti.html

• Общие рекомендации по безопасному использованию интернета и мобильной связи http://interneshka.org/students/gen_saf_rec.php

• Безопасный Интернет (рекомендации родителям) http://pcenter-tlt.ru/bezopasny-internet

• Поисковая система Яндекс Картинки https://yandex.ru/images