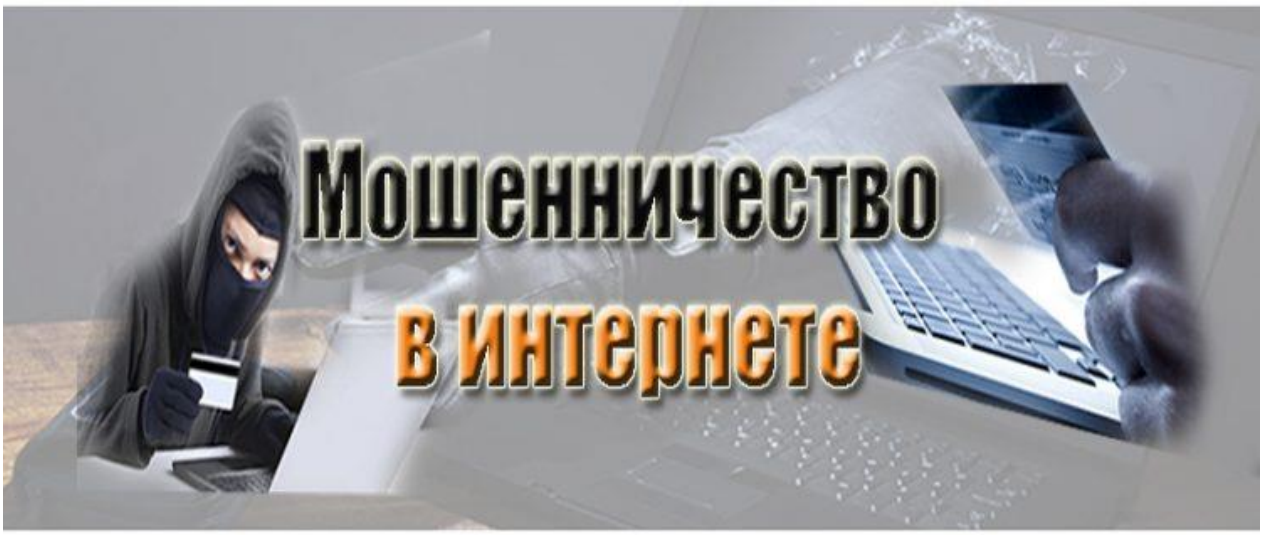
Муниципальное общеобразовательное учреждение

Средняя общеобразовательная школа №2 с.п.Атажукино

Индивидуальный итоговый проект на тему «Мошенничество в Интернете»



Работу выполнил:

Абсубаев Амин Эльдарович

ученик 10 класса

МОУ СОШ №2 с.п.Атажукино

Руководитель:

Афашагова З.М.

2022 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Под мошенничеством подразумевают факт изъятия собственности (различных ценностей) у одного человека в пользу другого (мошенника) обманным путем. То есть преступник втирается в доверие к пострадавшему и под «весомым» предлогом выманивает деньги или прочие ценности. Подобная деятельность преследуется законом. В «виртуальной» среде – это правило работает точно так же. Нельзя у человека выманить деньги и исчезнуть! Это тоже является преступлением!

Всем известно, что среднестатистический пользователь в большинстве случаев ищет информацию, скачивает музыку и фильмы, пишет в блог, посещает развлекательные сайты, пользуется почтой и т.п. Но вот однажды он сталкивается с заманчивым предложением заработать определенную сумму денег за короткое время. Неважно, что именно ему предлагают, в его голове уже начинают крутиться мысли о легком заработке. Даже если он достаточно осторожен и не доверяет всему, что пишут, качественный дизайн и грамотный текст могут развеять все его сомнения. Что уж говорить о неопытных подростках… Человек отсылает нужную сумму на кошелек или проводит какие-то другие действия, и терпеливо ждет. Мошенник же получает свои деньги.

Мошенничество в Интернете приобретает все большие масштабы. Изобретаются все новые уловки по вымоганию денег с простодушных пользователей. Практически полная безнаказанность, анонимность мошенников, большое количество доверчивых людей – все это подпитывает такой вот своеобразный вид получения прибыли.

Большинство пользователей просто забывают о том, что в Интернете действуют те же законы, что и в жизни. Сейчас редко найдешь человека, который бы попытался выиграть у наперсточника на вокзальной площади, а вот когда ему же предложат отослать деньги на так называемый «волшебный» кошелек, с тем, чтобы потом получить удвоенную сумму, все защитные психологические барьеры вдруг оказываются снятыми, и он с радостью соглашается. Все это напоминает 90-е годы, когда люди только после своего горького опыта (и чаще неоднократного) становились более осторожными, встречаясь с очередным предложением «легких» денег. В Интернете, как мы видим, «90-е» в самом разгаре…

Главное, что нужно помнить всем – «легких денег» не бывает. Никто никогда не даст денег просто так. Деньги не появляются из неоткуда, даже если они «электронные». А Интернет – это просто средство передачи информации.

Виды мошенничества в Интернете — это огромная проблема для современного мира. Дело в том, что компьютеры и всемирная паутина становятся основными источниками хорошего дохода людей. Таким образом, мошенники используют разные ходы, чтобы «развести» честных граждан.

Из-за того, что феномен Интернет-мошенничество в наше время обретает широкое распространение, а главное сильные социальные последствия, для нас представляется **актуальным изучение данного явления**.

В своей исследовательской работе я поднимаю следующий **проблемный вопрос:** какие правила необходимо 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 в Интернете; разработать рекомендации безопасного пользования ресурсами сети Интернет.

Задачи исследования:

- изучить основные виды мошенничества в сети Интернет;
- провести анкетирование по безопасному использованию сети Интернет среди учащихся;
- дать общие рекомендации по защите от мошенничества в сети Интернет.

В работе использованы такие **методы исследования** как исследование и обобщение.

Структура исследовательской работы представлена введением, тремя главами, заключением, списком использованной литературы и приложения.

Глава1. Основные виды Интернет-мошенничества

1.1. 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 выспрашиванием 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.

1.2. 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.

Все, наверное, видели, как время от времени при серфинге в Интернете внезапно появляются всплывающее окно или баннер с рекламой антивируса для вас? Иногда он выглядит как результаты уже проведенного сканирования вашего компьютера, в котором обнаружен десяток страшных вирусов. Чаще всего эти предупреждения и рекламы яркие, призывные. Однако не стоит поддаваться этому призыву! Фальшивый антивирус может причинить вам немало вреда. Меры, которые предлагает фальшивый антивирус, сами по себе правильные: сканирование на вирусы, обновление программ. Беда в том, что под видом обновлений в данном случае могут быть скачаны вредоносные программы. Основной задачей фальшивого антивируса является не поиск и уничтожение вирусов, а принуждение жертвы к оплате 1-3 тысяч рублей за «защиту», которая не работает. Возможны и другие варианты: поиск и похищение личной информации, в том числе банковской, списание денег с кредитной карты, а также порча файлов на компьютере.

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.

1.3. 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.

1.4. 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.

1.5. Работа на дому

В зависимости от того, насколько искушенным пользователем интернета является соискатель, а также от продолжительности поиска *надомной работы*, рано или поздно (вероятнее всего, что сразу) он сталкивается с огромным числом мошеннических предложений. Стоит только

приступить к изучению имеющихся вакансий - сразу создаётся впечатление, что существует масса профессий надомной работы, а также невостребованных рабочих мест, где можно зарабатывать деньги "дома", "в тапочках", особо себе не утруждая походами на работу. И, что немаловажно, при свободном графике работы и минимальной занятости предлагаются очень серьёзные деньги в качестве оплаты такому удаленному работнику.

Причём, во многих случаях требования к соискателям максимально лояльны, мало того, во многих вакансиях указывается, что никаких специфических знаний для выполнения работы не потребуется, иногда даже не нужно знать сколь-нибудь углубленно о компьютерах, будет предложена простая ручная работа в удобной обстановке с очень даже конкурентной оплатой.

К сожалению, приходится на сегодня констатировать факт наличия признаков мошенничества в очень большом их числе (примерно 97-98% вакансий надомной работы являются мошенничеством). Искушенные пользователи (те, кто далеко не первый день занимается удаленной работой или её поиском) признаки мошенничества определяют по первым строчкам таких предложений.

В Интернете огромная масса предложений о так называемой работе на дому, за которую вам обещают платить хорошие деньги. Но на самом деле в большинстве случаев вы будете работать бесплатно, а некоторые сомнительные работодатели, предлагающие такую работу, будут пытаться с вас выманить деньги. Такие предложения о работе, как правило, связаны с набором текстов, переводом текстов, сортировкой изображений, рассылкой писем, выращивания грибов, изготовлением мыла ручной работы и так далее.

Чтобы работать на дому и гарантированно получать за это оплату, необходимо обращаться на биржу фриланса (это специальные сервисы в Интернете). Только там действительно можно зарабатывать, причем неплохо. Также есть много других способов заработка, но это уже работа в Интернете, хотя ее можно назвать и работой на дому.

1.6. 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 все 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.

1.7. Вишинг

Еще один вид мошенничества – Вишинг (vishing — **v**oice ph**ishing**) назван так по аналогии с фишингом — распространённым сетевым мошенничеством. Сходство названий подчеркивает тот факт, что принципиальной разницы между вишингом и фишингом нет. Основное отличие **вишинга** в том, что так или иначе задействуется телефон.

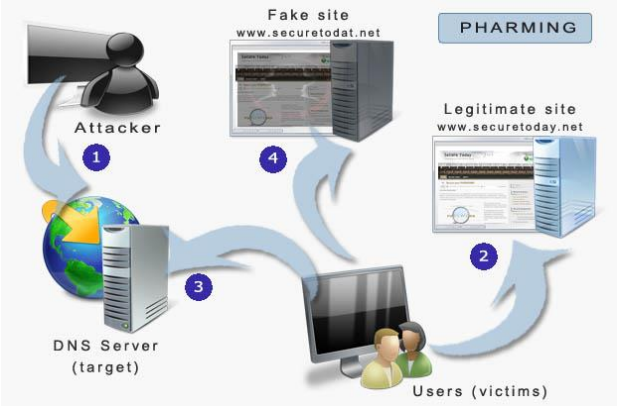
Типичный пример **фишинга**, когда клиенты какой-либо платёжной системы получают сообщения по электронной почте якобы от администрации или службы безопасности данной системы с просьбой указать свои счета, пароли и т.п. При этом ссылка в сообщении ведёт на поддельный сайт, на котором и происходит кража информации. Сайт этот уничтожается через некоторое время, и отследить его создателей в интернете достаточно сложно.

Схемы обмана в случае **вишинга** те же самые. Только в случае **вишинга** в сообщении содержится просьба **позвонить на определённый городской номер**. При этом зачитывается сообщение, в котором потенциальную жертву просят сообщить свои конфиденциальные данные. Например, ввести номер карты, пароли, PIN-коды, коды доступа или другую личную информацию в тоновом наборе.

Первые эпидемии **вишинга** зафиксированы в 2006 году.

Чтобы избежать обмана, достаточно знать тоже самое, что и в случая фишинга.

1.8. Фарминг



Еще один вид мошенничества – Фарминг. Он более эффективный, по сравнению с фишингом. **Фарминг** (англ. *pharming*) — это процедура скрытного перенаправления жертвы на ложный IP-адрес.

В классическом фишинге злоумышленник распространяет письма электронной почты среди пользователей социальных сетей, онлайн-банкинга, почтовых веб-сервисов, заманивая на поддельные сайты пользователей, ставших жертвой обмана, с целью получения их логинов и паролей. Многие пользователи, активно использующие современные веб-сервисы, не раз сталкивались с подобными случаями фишинга и проявляют осторожность к подозрительным сообщениям. В схеме классического фишинга основным "слабым" звеном, определяющим эффективность всей схемы, является зависимость от пользователя – поверит он фишеру или нет. При этом с течением времени повышается информированность пользователей о фишинговых атаках. Банки, социальные сети, прочие веб-службы предупреждают о разнообразных мошеннических приемах с использованием методов социальной инженерии. Все это снижает количество откликов в фишинговой схеме – все меньше пользователей удается завлечь обманным путем на поддельный сайт. Поэтому злоумышленники придумали механизм скрытого перенаправления пользователей на фишинговые сайты, получивший название фарминга ("pharming" – производное от слов "phishing" и англ. "farming" – занятие сельским хозяйством, животноводством). Злоумышленник распространяет на компьютеры пользователей специальные вредоносные программы, которые после запуска на компьютере перенаправляют обращения к заданным сайтам на поддельные сайты. Таким образом, обеспечивается высокая скрытность атаки, а участие пользователя сведено к минимуму – достаточно дождаться, когда пользователь решит посетить интересующие злоумышленника сайты.

Способов абсолютной защиты от фарминг-атак не существует, поэтому необходимо использовать профилактические меры:

- Использовать и регулярно обновлять лицензионное антивирусное программное обеспечение.
- Использовать защиту электронного почтового ящика (отключить предварительный просмотр).
- Не открывать и не загружать вложения электронных писем от незнакомых и сомнительных адресатов.

1.9. Кардинг

Кардинг - **в**ид 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.

Глава 2. Наказание за мошенничество в Интернете

Большинство интернет мошенников, начиная свою деятельность, уверены в своей полной безнаказанности. Многим кажется, что в глобальной сети можно сохранить анонимность, а правовая безграмотность обычных интернет-пользователей не позволит им наказать обидчиков. На самом деле, ситуация не так проста, и ответственность за совершённые в сети преступления всё-таки предусмотрена.

Если вы столкнулись с мошенничеством в Интернете, то жаловаться следует туда же, куда обращаются в случае обычного хищения, — в правоохранительные органы. Не стоит думать, что раз вы не знаете мошенника в лицо, то дело безнадежно. За время существования во Всемирной паутине мошенничества правоохранительные органы приобрели достаточный навык расследования подобных дел. Не стоит отказываться от подачи жалобы и по причине небольшой суммы похищенных денег. Вполне возможно, что ваша жалоба будет далеко не первой, и сведения, сообщенные именно вами, помогут вывести злоумышленников на чистую воду.

Куда обращаться при мошенничестве в Интернете конкретно? Всеми делами, связанными с компьютерной информацией, в системе МВД занимается отдел «К». Для более быстрого реагирования можно подать заявление непосредственно в региональное управление «К», однако вполне достаточно и просто написать жалобу в отделение полиции по месту жительства — сотрудники полиции сами направят ее по подведомственности.

При написании заявления нужно указать все имеющиеся у вас данные о мошенниках, в частности:

- адрес мошеннического сайта;
- ник злоумышленника на форуме;
- номер счета или электронного кошелька, на который были переведены денежные средства;
- номер телефона, на который было отправлено СМС-сообщение;
- адрес электронной почты мошенника и т. д.

Надо отметить, что подать жалобу можно и анонимно (в том числе устно по телефону горячей линии). Но практика показывает, что подобные заявления рассматриваются с меньшим энтузиазмом. Кроме того, согласно УПК РФ, анонимное заявление не может стать непосредственным поводом для возбуждению дела.

Подать жалобу на мошенничество в Интернете можно и в электронном виде — на сайте МВД. Для этого нужно заполнить специальную форму в разделе «Прием обращений». В таком случае жалобу следует адресовать непосредственно управлению «К».

Наш уголовный кодекс содержит ряд статей, карающих, в том числе и за мошенничество в интернете. В первую очередь, речь идёт о статье 159 «Мошенничество». В ней дано чёткое определение этого вида преступлений, а также предусмотрено соответствующее наказание. Итак, мошенничеством называется хищение чужой собственности или приобретение прав на неё с использованием обмана или со злоупотреблением доверием. Именно под эту статью УК можно «подвести» большинство случаев мошенничества в Интернете. И наказание за подобные нарушения предусматривает как штраф, так и обязательные или исправительные работы, арест, либо лишение свободы.

При совершении мошенничества в Интернете статья закона, по которой виновный понесет ответственность, зависит от стоимости похищенного и от обстоятельств хищения.

Если стоимость похищенного не более 2 500 тыс. руб., то мошенник подлежит административной ответственности по ст. 7.27 КоАП РФ. В качестве наказания эта норма предусматривает штраф, арест до 15 суток или обязательные работы.

Если мошенничество в Интернете совершено на сумму более 2 500 тыс. рублей, то оно является уголовно наказуемым. Квалификация преступления, то есть конкретная норма УК РФ зависит от способа мошенничества. Так, если имело место вмешательство в функционирование средств хранения и обработки информации (например, взлом аккаунтов в социальных сетях), речь пойдет о мошеннических действиях в сфере компьютерной информации — это ст. 159.6 УК РФ. Максимальным наказанием за подобные деяния является арест сроком на 4 месяца. Если же имеются отягчающие обстоятельства (совершение мошенничества группой лиц, хищение в

крупном или особо крупном размере и т. п.), то виновный может быть подвергнут заключению на срок до 10 лет.

Кроме того, мошенничество в Интернете попадает под действие ещё ряда статей уголовного кодекса. Например, деятельность злоумышленников может быть признана незаконным предпринимательством (статья 171 УК), уклонением от уплаты налогов (статья 182 УК), обманом потребителей (статья 200 УК) или же нарушением смежных и авторских прав (статья 146 УК). Существуют и специальные «компьютерные» статьи, карающие за неправомерный доступ к информации на компьютере (статья 272 УК), создание, распространение и использование вредоносного ПО (статья 273 УК), а также за нарушение правил пользования компьютером или сетью (статья 274 УК).

На мошеннический сайт можно пожаловаться на специальных сервисах, предназначенных для блокирования вредоносных сайтов. В частности, такие жалобы рассматриваются по следующим адресам:

- https://www.google.com/safebrowsing/report_phish/?hl=ru;
- http://virusdesk.kaspersky.ru/;
- https://analysis.avira.com/ru/submit-urls.

Кроме того, подать жалобу на компьютерное мошенничество можно на сайте Роскомнадзора (это орган по надзору в сфере информационных технологий).

Как видим, практически каждый из видов Интернет-мошенничества может быть наказан с помощью не одной, а нескольких статей УК.

Глава 3. Исследование уровня информационной безопасности обучающихся МОУ СОШ №2 с.п.Атажукино

В рамках исследования было проведено анкетирование с целью изучить уровень обучающихся по безопасному использованию сети Интернет. В социологическом опросе приняли участие 30 человек .

В ходе анкетирования были заданы следующие вопросы:

Анкета

1.Знаешь ли ты, что такое интернет-мошенничество? **Да \ нет**

2.Сталкивался ли ты в своей жизни с интернет-мошенничеством? **Да\ нет**

3.Если да, то с каким?_____

4.Знаешь ли ты, куда обращаться в случае такого мошенничества? **Да\ нет**

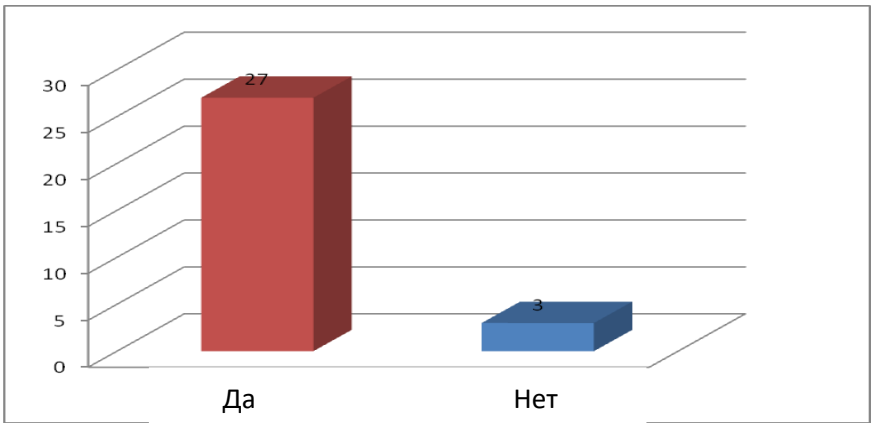
5. Обращался ли ты в такие органы? **Да\ нет\ хотел, но не знал куда**

6. Отвечаешь ли ты на сообщения коротких черных номеров? **Да\ нет**

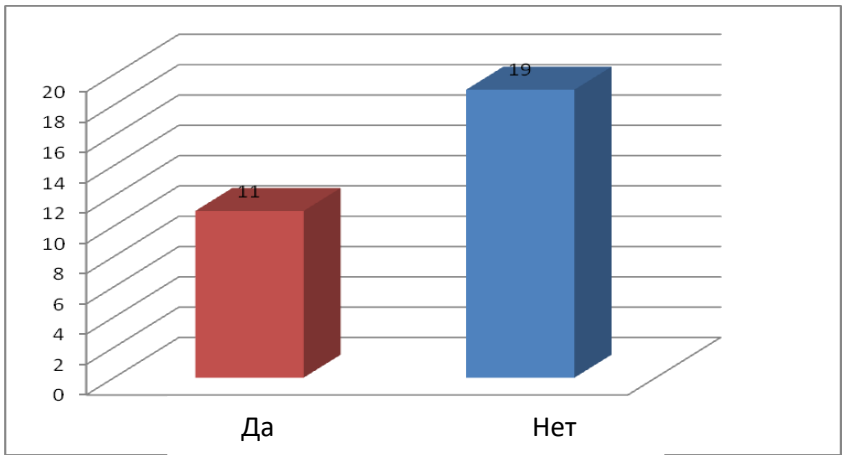
7. Подписывался ли ты на платные рассылки в интернете? И пострадал ли ты? **Да, но не пострадал/ Да, но пострадал/ Нет, не подписывался**

3.1. Итоги социологического опроса

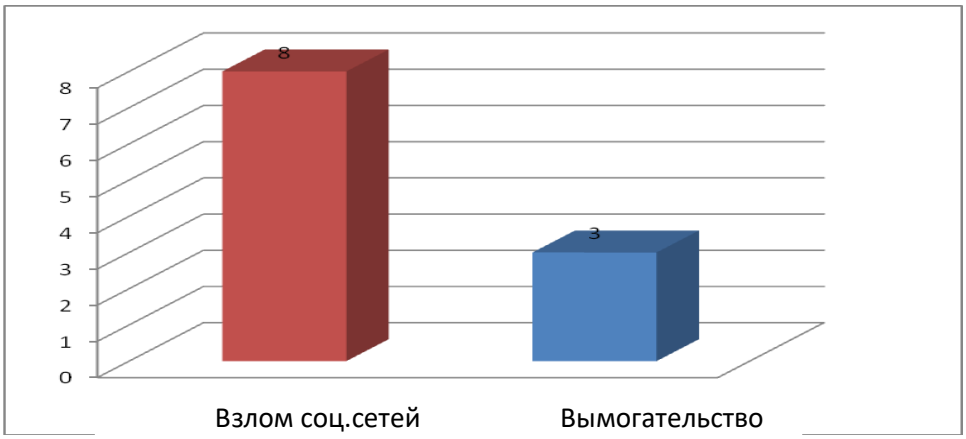
1. Знаешь ли ты, что такое интернет-мошенничество?



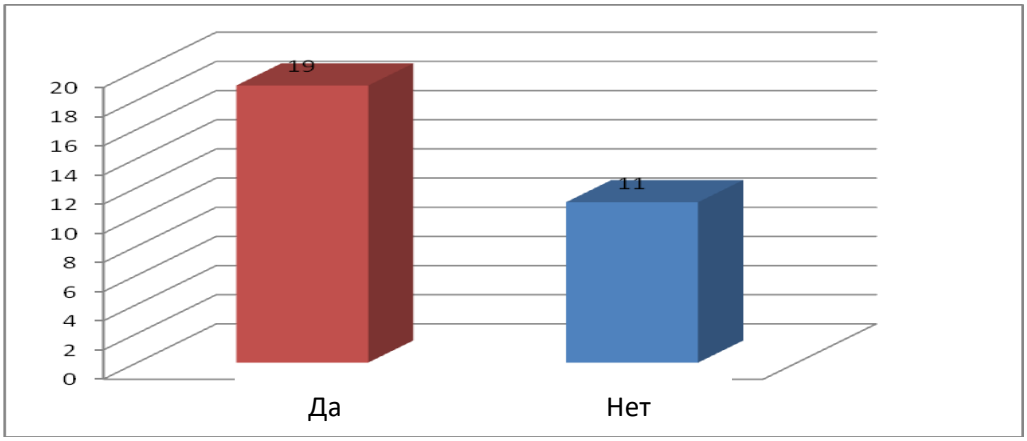
2.Сталкивался ли ты в своей жизни с интернет-мошенничеством?



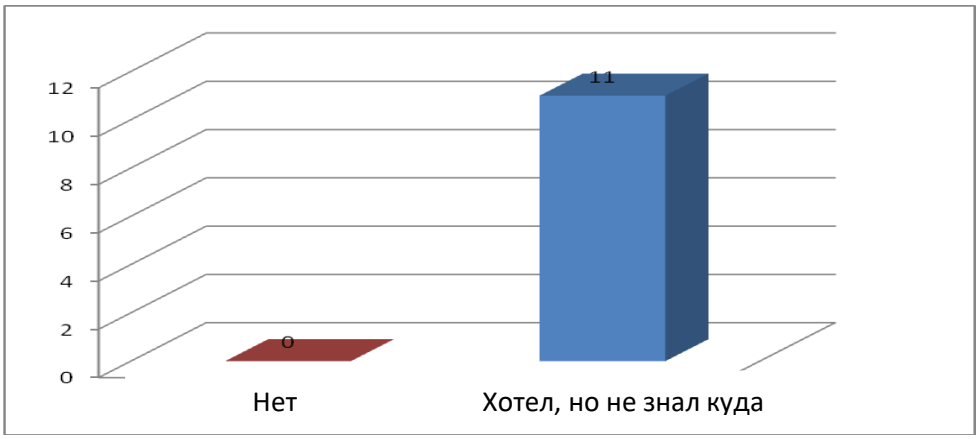
3. С каким видом Интернет-мошенничества ты столкнулся?



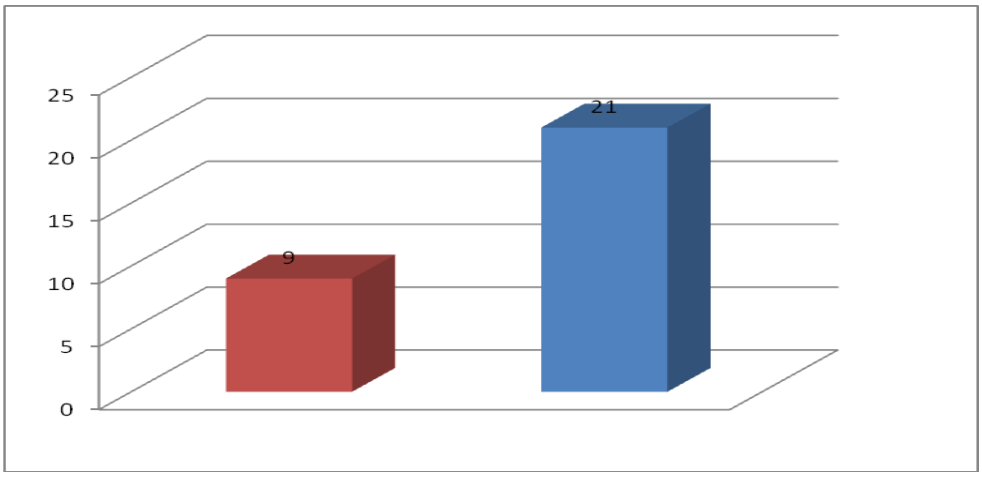
4. Знаешь ли ты, куда обращаться в случае такого мошенничества?



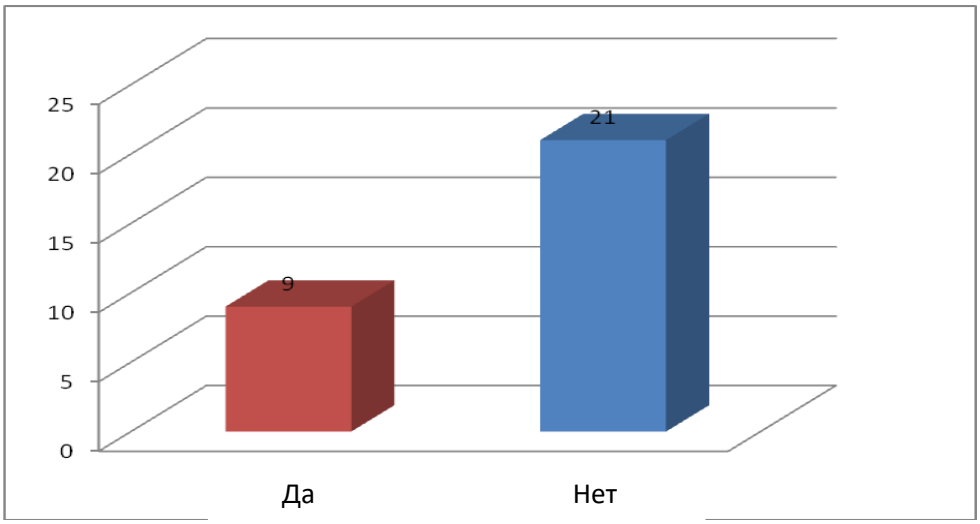
5. Обращался ли ты в такие органы?



6. Отвечаешь ли ты на сообщения коротких черных номеров?



7. Подписывался ли ты на платные рассылки в интернете?



Выводы:

- 90% опрошенных учеников и учителей имеют представление об Интернет-мошенничестве.
- 37% респондентов хотя бы раз в жизни сталкивались с виртуальными мошенниками.
- Чтобы работа в сети Интернет была безопасной, необходимо знать и соблюдать определённые правила.
- Необходимо познакомить с этими правилами как можно большее число людей.

Запомните основные признаки мошенничества в Интернете:

- Слишком сладкие обещания, например, вам предлагают получать нереально высокий доход за какую-то ерундовую работу.
- Отсутствие контактных данных на сайте для обратной связи, иногда они есть, но не действуют.

- Сайт, предлагающий Вам высокий дополнительный доход, сам расположен на бесплатном хостинге.
- Заманчивое предложение пришло к Вам на почтовый ящик в виде СПАМа.
- Просьба выслать или перевести на электронный кошелёк деньги за регистрацию, за инструкции, за почтовые расходы и т. п.
- SMS-оплата на короткий номер. В результате с баланса Вашего телефона снимут сумму в несколько сотен.

3.2. 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 за 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. Мы надеемся, что предоставленная информация будет вам полезна.

В исследовательской работе я представил 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, мы пришли к выводам, что не каждый знает об опасностях, подстерегающих их на просторах сети Интернет. Нашей задачей являлось выявить и устранить этот пробел в знаниях студентов. На мой взгляд, мы с ней справились.

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.

И еще. Не так давно в Интернете появилась любопытная страничка: “Предлагаем энциклопедию всех-всех-всех известных в мире Интернет-мошенничеств. Прочитав эту книгу, вы сможете противостоять жуликам и никогда не попадетесь в их сети!”. Ее авторы просят лишь перечислить на их электронный кошелек 10 рублей, и тогда вам укажут путь, по которому можно ее скачать на свой компьютер. Так что можете попробовать. По крайней мере, если вас и на этот раз (не дай бог!) обманут, это будет самой красивой аферой за всю историю Интернета.

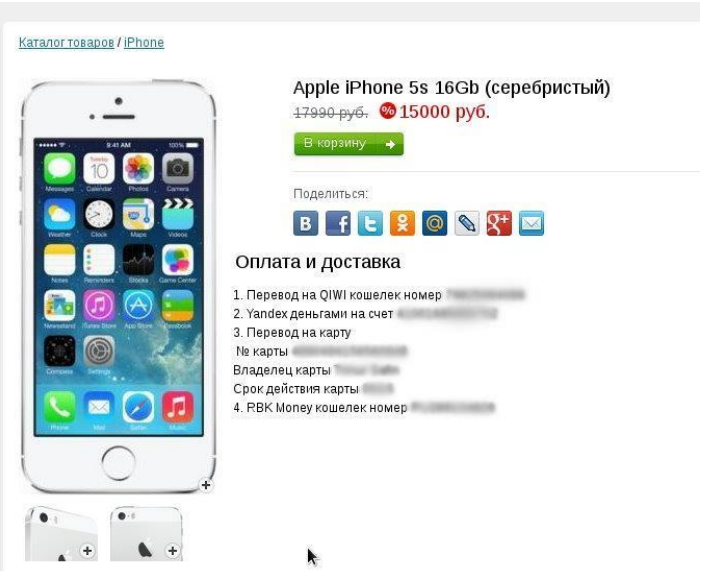
Список использованной литературы

1. Безопасный Интернет (рекомендации родителям) http://pcenter-tlt.ru/bezopasny-internet
2. Бизнес статьи «Каким бывает мошенничество в интернете?» https://businessman.ru/new-kakim-byvaet moshennichestvo-v-internete.html
3. Общие рекомендации по безопасному использованию Интернета и мобильной связи http://interneshka.org/students/gen_saf_rec.php
4. Способы обмана в глобальной сети http://consumersjournal.org/moshennichestvo/sposoby -obmana-v-globalnoj-seti.html

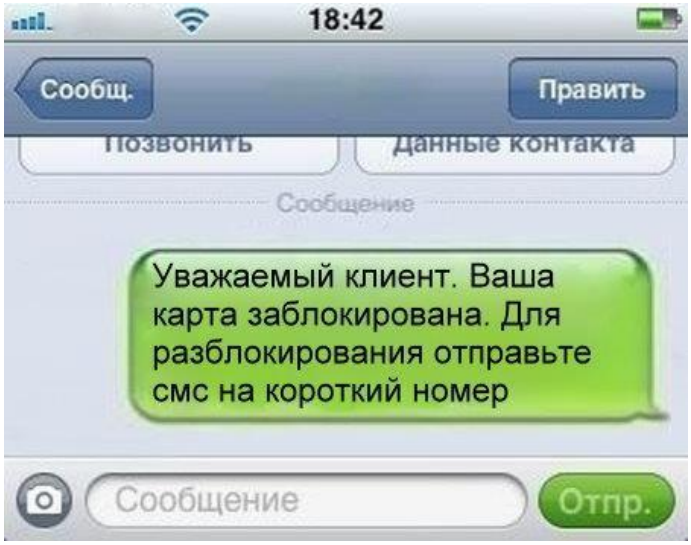
Приложение 1

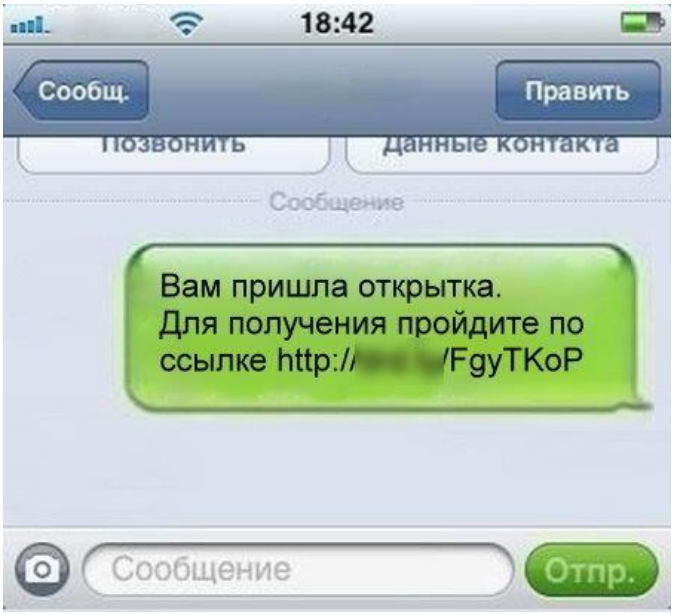
Памятка «Безопасный Интернет»

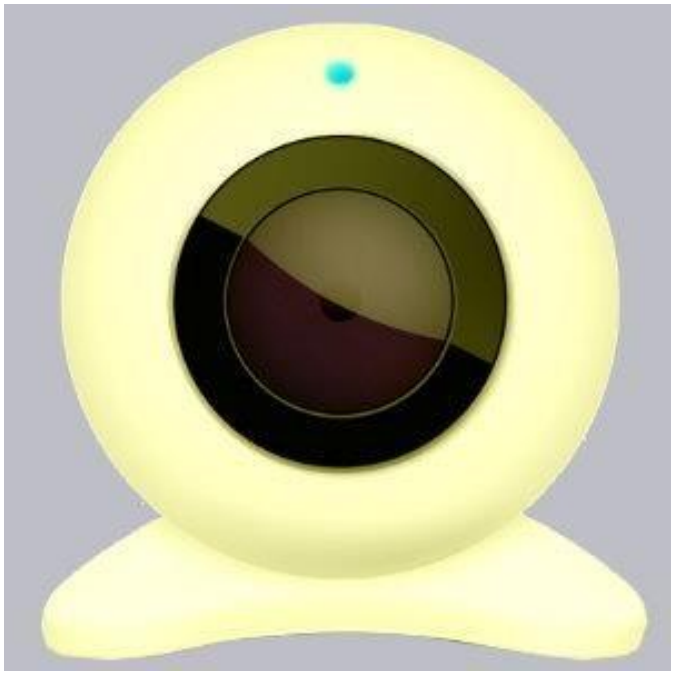
<table>
<tr><th colspan="2">СИТУАЦИЯ 1</th></tr>
<tr><td> 
</td><td>Вы получили электронное сообщение о том, что вы выиграли автомобиль и вас просят перевести деньги для получения приза?

НИКОГДА не отправляйте деньги незнакомым лицам на их электронные счета.
Помните, что вероятность выиграть приз, не принимая участия в розыгрыше стремится к нулю, а вероятность возврата денег, перечисленных на анонимный электронный кошелек злоумышленников, и того меньше.</td></tr>
<tr><th colspan="2">СИТУАЦИЯ 2</th></tr>
<tr><td> 
</td><td>Вы решили купить в интернет-магазине новый мобильный телефон, ноутбук или фотоаппарат по суперпривлекательной цене, но магазин просит перечислить предоплату?

НИКОГДА не перечисляйте деньги на электронные кошельки и счета мобильных телефонов.
Помните о том, что интернет-магазин не может принимать оплату за покупку в такой форме. Если вас просят оплатить товар с использованием терминалов экспресс-оплаты или перевести деньги на электронный кошелек, вероятность того, что вы столкнулись с мошенниками крайне высока.</td></tr>
</table>

СИТУАЦИЯ 3	
	Вы получили смс-сообщение о том, что ваша банковская карта заблокирована? **НИКОГДА не отправляйте никаких денежных средств по координатам, указанным в сообщении, не перезванивайте на номер, с которого оно пришло, и не отправляйте ответных смс.** *Самым правильным решением в данной ситуации будет позвонить в банк, выпустивший и обслуживающий вашу карту. Телефон банка вы найдете на обороте вашей карты.*
СИТУАЦИЯ 4	
	На электронной доске объявлений или в социальной сети вы нашли товар, который так долго искали, и стоит он намного дешевле чем в других местах? **НИКОГДА не перечисляйте деньги на электронные кошельки, не убедившись в благонадежности контрагента.** *Внимательно посмотрите его рейтинг на доске объявлений, почитайте отзывы других покупателей, поищите информацию о нем в сети Интернет. Подумайте над тем, почему товар продается так дешево, узнайте какие гарантии может предоставить продавец.*

СИТУАЦИЯ 5	
	Вы хотите приобрести авиабилеты через Интернет? **НИКОГДА не пользуйтесь услугами непроверенных и неизвестных сайтов по продаже билетов.** *Закажите билеты через сайт авиакомпании или агентства, положительно зарекомендовавшего себя на рынке. Не переводите деньги за билеты на электронные кошельки или зарубежные счета. При возникновении подозрений обратитесь в представительство авиакомпании.*
СИТУАЦИЯ 6	
	Вы получили СМС или ММС сообщение со ссылкой на скачивание открытки, музыки, картинки или программы? **НИКОГДА не переходите по ссылке, указанной в сообщении.** *Помните, что перейдя по ссылке вы можете, сами того не подозревая, получить на телефон вирус или оформить подписку на платные услуги.* *Даже если сообщение пришло от знакомого вам человека, убедитесь в том, что именно он является отправителем.*

СИТУАЦИЯ 7	
	Общаетесь в интернете и имеете аккаунты в соцсетях? **НИКОГДА не размещайте в открытом доступе и не передавайте информацию личного характера, которая может быть использована во вред.** *Общение в сети в значительной мере обезличено, и за фотографией профиля может скрываться кто угодно. Помните о том, что видео и аудиотрансляции, равно как и логи вашей сетевой переписки, могут быть сохранены злоумышленниками и впоследствии использованы в противоправных целях.*