**муниципальное бюджетное общеобразовательное учреждение**

**города Ростова-на-Дону «Школа № 6**

**имени Героя Советского Союза Самохина Н.Е.»**

**ИНДИВИДУАЛЬНЫЙ ПРОЕКТ**

на тему:
«Интернет-мошенничество и защита от него»

Выполнил учащийся 11А класса:
 Горбанев Денис Дмитриевич
 Научный руководитель:
 Басков Николай Николаевич

 Допуск к защите: \_\_\_\_\_\_\_\_\_

город Ростов-на-Дону- 2022год

 **Оглавление**

**Введение..................................................................................................3**

**История интернет-мошенничества.................................................................4**

**Влияние мошенничества на пользователей интернета...................5**

**Виды интернет-мошенничества.........................................................6-8**

**Расследование случаев интернет-мошенничества правоохранительных органов …......................................................................................................9**

**Рекомендации по пользованию интернетом...............................................10**

**Заключение........................................................................................................11**

**Список литературы.........................................................................................12**

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 проблемы:

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.

Проблемный вопрос:

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

Гипотеза исследования:

Избежать обмана в сети вполне вероятно, если пользователи будут хорошо проинформированы.

 ГЛАВА 1

1.1 История интернет-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 Интернет

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.

 **Глава 2 Виды мошенничества**

1.Ложные сайты

Создание ложных интернет-сайтов в настоящее время является одним из основных видов мошенничества, совершаемых посредством использования сети Интернет, который является самой большой торговой площадкой в мире, с не ограниченным территориальным пространством. Огромное количество торговых площадок, посредством которых у потребителя имеется возможность выбрать себе товар на разных площадках и приобрести его по низкой цене, оплатив безналичным расчетом, дает злоумышленникам возможность создавать сайты-двойники известных торговых платформ при помощи фарминга.

При совершении фиктивной покупки покупатель перечисляет свои деньги мошеннику, либо передает конфиденциальные данные своей банковской карты.

Как правило фиктивные ресурсы очень быстро прекращают свою работу, и установить владельца данного ресурса сложно в силу того, что регистрация сайта осуществляется дистанционно и полностью анонимно, поэтому даже спец. службы бывают бессильны.

2.Вредоносные программы

Другой разновидностью дистанционного мошенничества, является создание вредоносных программ, с помощью которых похищаются персональные данные пользователей. Вредоносные программы устанавливаются на электронные гаджеты с целью получения доступа к данным о банковских картах и счетах пользователей.

Возможность бесконтактной оплаты, напрямую связанная с закреплением в устройствах сведений о банковских картах и счетах, предоставляет мошенникам создавать и под различными предлогами принуждать потерпевших устанавливать данные программы на свои устройства. После установки, программа, заполучив необходимые сведения, через Интернет передает необходимые данные злоумышленнику, который получает доступ к финансам потерпевшего и распоряжается ими по своему усмотрению.

3. Похищение персональных данных

В отличии от предыдущего вида, похищение персональных данных может использоваться и из хулиганских побуждений, с целью повреждения используемого устройства. Похищение же персональных данных может сопровождаться и похищением сведений, порочащих честь и достоинство лиц. Ярким примером такого преступления является похищение фотографий личного содержания звезд кино и эстрады. Злоумышленники, заполучив подобного рода компрометирующие сведения, начинают шантажировать жертву, требуя денежных переводов под угрозой публикации полученных сведений.

Фиктивные сделки

Оформление фиктивных сделок с помощью Интернет-ресурсов, связано прежде всего с различными сферами жизни общества, как правило купли-продажи товаров и вещей или покупки чего-либо в интернет-магазине. При таком способе обмана злоумышленник получает от жертвы денежные средства, под предлогом предоплаты или оплаты доставки, а после либо не отвечает, либо исчезает.

Основным видом мошенничества является **фишинг**. Фи́шинг (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 поддержки сайт 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.

**2. Расследование случаев интернет-мошенничества правоохранительных органов**

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.

Что бы получить более подробную информацию по этой теме, я обратился в местное отделение полиции. Там мне пояснили, что 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. 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.

***Наказание:***
***- штраф до 120 000 рублей;***
***- штраф в виде годового дохода обвиняемого;***
***- принудительные работы до 180 часов;***
***- исправительные работы на 6-12 месяцев;***
***- арест на 2-4 месяца;***
***- лишение свободы на 2 года.***

Кроме того, мошенничество в интернете попадает под действие ещё ряда статей уголовного кодекса.

-Статья 171. Незаконное предпринимательство.

- Статья 182. Заведомо ложная реклама.

- Статья 199. Уклонение от уплаты налога.

-Статья 200. Обман потребителей.

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).

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

Исследование глобальных экономических преступлений, проведенное с участием деловых кругов в 78 странах, выяснило, что интернет - мошенничество занимает четвертое место в мире по частоте совершения.

Краткие рекомендации по безопасному использованию Интернетом

Подводя итоги, я решил сделать памятку, какие действия нельзя совершать в сети интернет:

* Регулярно обновляйте антивирусную программу на домашнем компьютере.
* Не сообщайте реквизиты банковской карты неизвестным.
* Будьте бдительны при вводе паролей и личных данных на сайтах, при переходе по незнакомым ссылкам.
* Не вводите данные банковской карты с компьютеров общественного пользования.
* Не открывайте подозрительные ссылки из писем и sms от незнакомых отправителей.
* Помните, что ни один из платежных сервисов не требует оплаты комиссии от получателя перевода.
* Ни в коем случае не верьте в возможность легкого заработка в сети Интернет.
* Получайте максимально полную и достоверную информацию о продавце или интернет - магазине перед покупкой товара и не приобретайте ничего в социальных сетях**.**

**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. Итак, я рассмотрел определение мошенничества, определил его характеристики и выделил те статьи в УК РФ, по которым можно привлечь Интернет-мошенников к ответственности. Проанализировав сообщения мошенников, а также информационную базу, касающуюся мошенничества в Интернете, выделил типологии Интернет - мошенничества: по методике исполнения, по каналам коммуникации, по сфере воздействия, по коммуникативным средствам. Привела примеры типологии мошенничества в сети - Интернет. На мой взгляд, описано большинство основных форм мошенничества, у них есть общая черта - попытка выудить у пользователя деньги.

В заключение работы предлагаю несколько практических рекомендаций. Я бы посоветовала пользователям расширять знания касательно возможностей Интернета, а главное, особенностей виртуального пространства, в силу которых неосведомленный пользователь оказывается уязвимым перед мошенниками. Необходимо создавать вебсайты, посвященные информированию пользователей Рунета об основных техниках мошенничества. Информация того же рода должна освещаться в СМИ. Правоохранительным органам необходимо законодательно урегулировать меры ответственности за виртуальное мошенничество, вводить больше органов по контролю за безопасностью в Интернете и практиковать наказания Интернет - мошенников.

**Список использованной литературы**

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