**Муниципальное бюджетное общеобразовательное учреждение**

**«Гимназия №32» города Кургана**

# ТВОРЧЕСКО-ИССЛЕДОВАТЕЛЬСКИЙ ИНДИВИДУАЛЬНЫЙ ПРОЕКТ

## Финансовое мошенничество в Интернете

Секция: Обществознание

Автор:

Кудрин Глеб Евгеньевич

10 Ф класс

Руководитель:

Титевалова Ирина Николаевна,

учитель обществознания

г. Курган, 2022

# СОДЕРЖАНИЕ

## 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.

## Цель:

Проинформировать людей о проблеме финансового мошенничества, указать способы его решения и предотвращения.

## Задачи:

1) Изучить виды финансового мошенничества;

2) Выработать стратегию грамотного поведения в ситуациях растущих финансовых рисках;

3) Научиться применять полученную информацию на практике.

## Средства решения:

1. Теория, дополнительная информация;
2. Опрос;
3. Анализ.

## Гипотеза:

Если уровень финансовой грамотности среди населения будет расти, то количество людей, попавшихся на махинации аферистов, уменьшится.

# Теоретическая часть

# Понятие и значение термина «Финансовое мошенничество»

**Финансовое мошенничество -** это преступление, совершенное в сфере экономики и направленное против собственности. Мошенничество представляет собой хищение чужого имущества или приобретение прав на чужое имущество путем злоупотребления доверием или обмана. При этом под обманом понимается как сознательное искажение истины (активный обман), так и умолчание об истине (пассивный обман).
В обоих случаях обманутая жертва сама передает свое имущество мошеннику.

## Финансовое мошенничество в Интернете

Термин «**финансовое мошенничество в Интернете**» применим в целом к мошенническим махинациям любого вида, где используются один или несколько элементов Интернета – электронное мошенничество: попрошайничество; фиктивная работа на дому; фиктивные Интернет-магазины; фиктивные платежные системы; мошенничество в социальных сетях и электронной почте; спам и вирусные вымогательства (рассылки с требованием выкупа); фиктивный обмен валют и другие операции на рынке ценных бумаг; оплата информационных услуг с помощью СМС сообщений и др.. Если вы достаточно часто пользуетесь Интернетом, вы вскоре заметите, что события и операции в виртуальном мире обычно совершаются «в режиме Интернет-времени». Для большинства людей это выражение означает только, что в Интернете все, как представляется, совершается быстрее – деловые решения, поиск информации, личное взаимодействие и многое другое – и происходит до, в течение или после обычного рабочего времени в реальном мире. К сожалению, мошенники в Интернете тоже действуют «в режиме Интернет-времени». Они стремятся максимально использовать уникальные возможности Интернета – такие как рассылка электронных сообщений за несколько секунд по всему миру или размещение информации на веб-сайте, так что она становится доступна всему миру, для проведения различного рода махинаций намного быстрее, чем раньше.

# 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.

## 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.

## 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.

## 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.

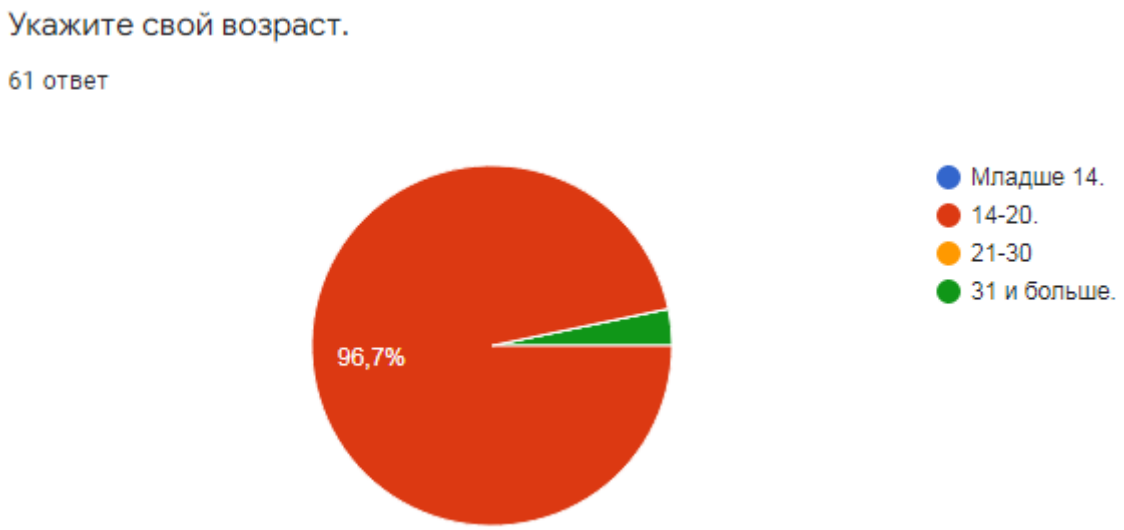
Все? Как бы не так! Дело в том, что с вашего лицевого счета была списана отнюдь немаленькая сумма! Более того, она может продолжать списываться через определенное время. Это так называемая подписка, от которой нужно отписаться. Для этого надо отправить слово STOP или СТОП на четырехзначный номер, который вы можете узнать у своего оператора связи.

# Практическая часть

## 2.1 Социальный опрос. Анализ данных. Вывод

Я создал социальный опрос с помощью Google Диска, где использовал 4 вопроса, которые четко дали мне ответ на поставленный вопрос.

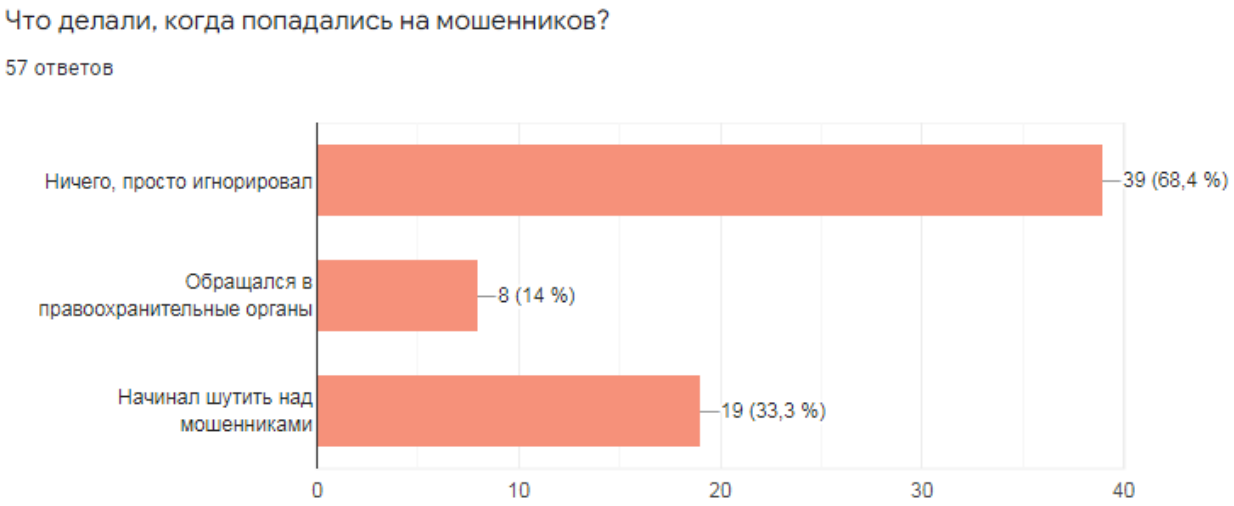
В первом вопросе мне было важно узнать возраст участников опроса. Но не с целью проверить, люди какой возрастной категории больше сталкивались с мошенниками, а для того, чтобы проверить, кого заинтересовал этот опрос.





Данный вопрос доказал актуальность моей темы и смысл дальнейшего исследования. Также на диаграмме наглядно показано, что каждый отвечающий слышал или знает о понятии «мошенничество».


Третий вопрос показал, что большинство (80%) прошедших опрос никогда не попадались на уловки мошенников. Также этот вопрос подтверждает мою гипотезу о том, что **если уровень финансовой грамотности среди населения будет расти, то количество людей, попавшихся на махинации аферистов, уменьшится.**




По данной статистике последнего вопроса из моего опроса, большинство ответивших на последний вопрос просто начинали игнорировать мошенников. Но 8 человек все-таки обращались в полицию, я думаю это те люди, которые попались на уловки и добровольно отдали свои деньги в руки мошенников.

## Выводы:

- 100% опрошенных учеников имеют представление об Интернет-мошенничестве.
- 50% 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.

## Рекомендации по безопасному использованию ресурсов сети Интернет:

- 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.
- 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!

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

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 использованной литературы


1) http://pcenter-tlt.ru/bezopasny-internet
2) https://businessman.ru/new-kakim-byvaet
3) http://interneshka.org/students/gen_saf_rec.php
4) http://consumersjournal.org/moshennichestvo/sposoby -obmana-v-globalnoj-seti.html