Научно-исследовательская работа

по обществознанию

«Финансовое мошенничество в интернете»

Выполнили:
Внук Каролина Сергеевна
учащаяся 8 класса
Яковлева Анна Андреевна
Учащаяся 8 класса
МОБУ «Сясьстройская школа № 2, Россия, г.Сясьстрой

Руководитель:

Басырова Ирина Николаевна,

Учитель истории и обществознания

МОБУ «Сясьстройская школа № 2, Россия, г.Сясьстрой

Оглавление

Введение

Данная работа посвящена проблеме распространения финансового мошенничества в Интернете. В наше время она как никогда актуальна, так как финансовое мошенничество в Интернете приобретает все большие масштабы. 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.

Изобретаются 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.

Как известно, средствами получения денег является либо производство товаров, либо предоставление услуг. Для Интернета данное утверждение звучит так: либо вы получаете прибыль с производства интеллектуальной собственности, либо с предоставления сопутствующих услуг....

Практическая значимость проекта: полученные данные могут использоваться для обеспечения личной безопасности в сети Интернет.

Теоретическая значимость: данная работа может явиться вкладом в исследование современного информационного общества и опасностей сети Интернет.

Проблема: мошенничество является одной из основных угроз финансовой безопасности граждан.

Цель работы: повышение уровня финансовой грамотности обучающихся МОБУ « Сясьстройская СОШ № 2»

Задачи:

1.Познакомиться с понятием финансового мошенничества

2.Определить виды финансового мошенничества

3.Изучить виды интернет-мошенничества

4.Выработать советы по безопасному использованию Интернет-ресурсов

1.1. Понятие финансового мошенничества и его виды

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.

Виды финансового мошенничества:

1. Мошенничество с материнским капиталом.
2. Финансовая пирамида.
3. Продажа изделий медицинского назначения, которые излечивают неизлечимые болезни.
4. Мошенничество при помощи мобильной связи.
5. Автоподстава.
6. Мошенничество в сети «Интернет»

1.2. 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.

1.3. Махинации, связанные с интернет- магазинами

В интернет-магазинах можно приобрести что угодно. Чтобы не попасться на удочку мошенников, нужно соблюдать элементарные правила осторожности. Отсутствие телефона, фактического адреса продавца или слишком низкая цена на товар, скорее всего, свидетельствует о том, что покупателю подсунут подделку или просто присвоят его деньги. Если на сайте магазина указан телефон, не поленитесь позвонить и подробно расспросить о характеристиках и особенностях товара. Неверная информация или заминки со стороны продавца должны стать серьезным поводом для отказа от покупки.

Примером махинации мошенников в интернет магазинах может послужить случай 24-летней жительницы Приморского района. Она на одном из сайтов в сети Интернет поместила объявление о продаже детских вещей. Вскоре откликнулся покупатель. Он обрадовал предложением покупки и попросил продавца сообщить реквизиты банковского счета для перечисления на него денежных средств. Выяснив данные, злоумышленник похитил с банковской карты потерпевшей 13 тысяч рублей.

Фишинг

Фишинг (от англ. fishing - рыбная ловля)–очень распространенный вид мошенничества, целью которого является получение данных, содержащихся на пластиковой карте. Пользователям рассылаются письма по электронной почте от имени платежных систем или банков об изменении систем безопасности или другими предлогами. Мошенники создают сайты-двойники, в точности копирующие оригинал, куда и заходят ничего не подозревающие пользователи.

Для того чтобы иметь возможность в дальнейшем использовать пластиковую карту, на сайте-двойнике предлагается ввести данные, содержащиеся на карте и PIN-код. Эти данные потом

используются для изготовления поддельных пластиковых карт и снятия со счетов наличных денег в банкоматах. Одна из разновидностей фишинга – звонки на мобильный телефон клиента от якобы представителя банка с просьбой погасить накопившуюся задолженность по кредиту. Когда ничего не подозревающий гражданин пытается объяснить, что никакого кредита он никогда не брал, ему предлагают уточнить данные, которые содержит его пластиковая карта.

Для покупки товаров и услуг сама карта уже не нужна – достаточно данных, которые пользователь сам предоставил мошенникам. Пользователям любой платежной системы нужно помнить, что банки и другие кредитные и финансовые организации никогда не присылают электронных писем и не звонят с просьбой предоставить сведения, указанные на пластиковой карте. В случае если происходит какое-либо недоразумение, клиента всегда просят приехать в банк лично.

Кардинг

Кардинг является мошенничеством, также, как и фишинг, связанный с банковскими картами. Злоумышленники разнообразными способами пытаются узнать пароли и сведения, указанные на карте. С помощью этих данных мошенники впоследствии совершают покупки через Интернет или обналичивают деньги посредством поддельных пластиковых карт. Данные пользователей карт обычно получают путем создания подставных интернет-магазинов, которые ничего на самом деле не продают, а только занимаются сбором сведений с чужих пластиковых карт.

Фарминг

Фарминг, можно сказать, является более продвинутой версией фишинга. Смысл данного вида мошенничества в интернете заключается опять же в направлении пользователя на другой сайт. Но это делается

уже не через поддельные ссылки и т.д., а через заражение компьютера вредоносными программами или другими способами.

Финансовые пирамиды

Что такое финансовая пирамида? Это особая организация, которая предлагает вложить немного денег и через некоторое время получить крупную сумму. Достигается это за счет прихода новых вкладчиков, часть от взноса которых переходит на ваш счет. Чем больше после вас будет участников, тем больше вы заработаете. Самой известной на сегодняшний момент является финансовая пирамида МММ.

Казалось бы, что тут плохого вложил мало, получил много. Дело в том, что никто не знает, когда эта организация прекратит прием взносов. Последние вкладчики теряют свои деньги. Действительно зарабатывают только те, кто подключился к «строительству» в начале и в середине.

На данный момент в сети большое количество сайтов, которые предлагают вложиться в пирамиды, и заработать тысячи долларов, сделав взнос, не превышающий 10$. Это обман! Вы потратите деньги, а ресурс через некоторое время попросту исчезнет с просторов интернета, оставив вас с носом! Многие мошенники создают псевдо официальные сайты Сергея Мавроди (создателя МММ). Не верьте, последняя пирамида МММ прекратила свою деятельность в 2012 году и с тех пор больше не возобновлялась.

Еще одним особым видом финансовых пирамид является сетевой маркетинг. Не весь, конечно! А только MLM компании, которые предлагают покупать другим товар, который является, по сути, мусором. При этом они часто требуют оплаты вступительных взносов!

1.4. Трюки мошенников, приносящие финансовый вред

1. Продажа смартфона

В сфере онлайн продаж (частных) чаще всего обманывают покупателей. Но бывает так, что и продавцы попадают в ловушку. Например, при продаже айфона потенциальный покупатель может попросить проверить работу iCloud на этом телефоне (только тогда согласен купить). При проверке мошенник блокирует телефон, меняет пароль и вымогает деньги. Вообще к таким категориям относятся любые гаджеты, привязанные к учётной записи (в том числе Андроид).

2. Чудо-интернет-кошелёк

Периодически в интернете появляются «волшебные» онлайн кошельки. И если на такой кошелёк положить деньги, то через некоторое время сумма на нём удвоится или даже утроится (почти как в пирамиде) из-за ошибок программистов. И есть «добрые» люди, которые делятся номерами кошельков «по секрету» с другими. Разумеется, ничего подобного не существует, но люди верят в надежде получить халявные деньги.

3. Срочная продажа с большой скидкой

Контекстная реклама на сайте нередко может мелькать «очень выгодным предложением» купить что-то по большой скидке (вплоть до 90%). Пользователь переходит на сайт, регистрируется, оставляет свой номер телефона, на который достаточно быстро перезванивают и сообщают, что товар последний (из-за низкой цены всё разобрали) и будет продан тому, кто быстрее заплатит. Клиента просят сделать полную предоплату (и часто из-за страха упустить «супер выгодное предложение» он соглашается), и деньги улетают в неизвестном

направлении. Стоит ли говорить, что после этого никого товара не будет?

4.Редкий товар.

Есть в интернете сайты, на которых можно «найти» самые редкие товары, даже несуществующие. И купить можно прямо сейчас, да и с бесплатной доставкой — достаточно оплатить покупку онлайн. И деньги уплывают в небытие. Очень часто так продают редкие книги (вернее часто так обманывают доверчивых покупателей). Всегда проверяйте подлинность сайта, никогда не оплачивайте сразу покупку на таком сайте, поищите в интернете отзывы о нём (которые тоже нужно уметь фильтровать).

5. Деньги на благотворительность

В соц. сетях периодически мелькают посты с просьбой пожертвовать деньги куда-то или кому-то. При этом истории могут быть реальные (взяты с сайта благотворительной организации), но счёт, на который просят перевести деньги, может быть мошеннический. А как понять? Если просят перечислить деньги в фонд, то должны быть конкретные реквизиты организации (их подлинность можно легко проверить на их сайте), а не номер карты физического лица. Если деньги собирает частное лицо, то можно вступить с ним в онлайн диалог и с помощью направляющих вопросов понять, мошенник это или нет.

Одним из примеров таких махинаций является случай 24-летней жительницы Волгограда. Пострадавшая на одном из сайтов в сети Интернет поместила объявление о продаже детских вещей. Вскоре откликнулся покупатель. Он обрадовал предложением покупки и попросил продавца сообщить реквизиты банковского счета для перечисления на него денежных средств. Выяснив данные, злоумышленник похитил с банковской карты потерпевшей 13 тысяч рублей.

6. Фейковые центры финансовой грамотности

Из-за возросшего интереса к финансовой грамотности населения в условиях экономического кризиса появились так называемые «центры финансовой грамотности». На своих занятиях и в своих статьях они рассказывают, как пользоваться именно их услугой, как открыть у них счёт, как взять у них займ, как вернуть займ, как оформить кредитную карту, как покупать валюту с плечом, как заработать, если приведёшь друга и т.п. Это не про финансовую грамотность (хотя частично полезные аспекты присутствуют), это про продажу услуг, просто маркетинг.

7. Письма о псевдо долгах от мошенников

Федеральная служба судебных приставов (ФСПП) сообщает, что в интернете появились мошенники, которые представляясь судебными приставами, массово рассылают гражданам электронные письма с уведомлениями о псевдо долгах, в которых содержатся «ссылки на вредоносный код». В таких сообщениях якобы должника уведомляют, что в короткий срок требуется погасить долг для избежания ареста имущества неплательщика. Кроме того, мошенники предлагают кликнуть по ссылке для получения более полной информации о судебном решении по задолженности. После перехода по ссылке, система предлагает загрузить файл, который содержит в себе вирус, способный заразить компьютер, похитить или уничтожить важную информацию.

1.5. Как не попасться в «сети» аферистов

Будьте бдительны во время работы в интернете. В первую очередь это касается предложений отправки смс на короткие номера. Ловушек много: завлекающий контент (диеты, платные архивы и т.д.), элитные вакансии, закрытая биржа копирайтеров, где обещают баснословные суммы и т.д. Как только вы понимаете, что дело идет к отправке смс, то сразу пролистывайте веб-страницу вниз и ищите внизу условия оплаты, написанные мелким шрифтом. Цены вас поразят. Если же условий нет, то всегда можно проверить реальную стоимость отправки смс на короткие номера через специальные бесплатные сервисы.

1. При совершении покупок онлайн обращать внимание, применяется ли при оплате протокол 3D Secure. При использовании данного протокола каждый платеж с вашей банковской карты подтверждается не только вводом cvv2/cvc2 кода, но и паролем авторизации на домене эмитента карты. Этот пароль чаще всего приходит вам в виде смс-сообщения на мобильный телефон, указанный в договоре на выпуск платежной карты, при совершении оплаты и является одноразовым.

2. При расчете банковской картой важно убедиться, что система платежей отвечает требованиям международного стандарта безопасности данных индустрии платежных карт (PCI DSS). Требования данного стандарта направлены на обеспечение информационной безопасности платежей на всех уровнях. Соответствие PCI DSS организация обязана подтверждать ежегодно, что фиксируется сертификатом соответствия.

3. Использование платежным порталом SSL-сертификата гарантирует пользователю подлинность компании и данных, которые он получает от нее в процессе совершения оплаты. Благодаря криптографическому

протоколу клиент может быть уверен, что информация, которой он обменивается с сайтом, не может быть перехвачена, а также не подлежит изменению.

- Старайтесь не открывать по ссылке в письме сайты платежных систем. Обязательно проверяйте url в адресной строке или свойства ссылки. Внешне сайт-двойник может в точности копировать оригинал. Перед тем, как вводить на сайте данные, убедитесь, что сайт принадлежит именно этой платежной системе.

- Никогда и никому не сообщайте свои пароли и PIN-коды.

- Не храните файлы с конфиденциальной информацией на ненадежных или общедоступных носителях информации. Делайте несколько копий.

- Письма, в которых сообщается о проблемах с вашим счетом, в которых присутствует просьба перейти на сайт или произвести какие-либо действия, смело отправляйте в корзину. Помните! Техническая поддержка никогда таких писем не рассылает.

- Почти в 100% случаев платежи, которые вы делаете в сети, отменить уже нельзя. Прежде чем оплатить товар или услугу, все внимательно проверьте.

1.6. Чтобы не стать жертвой мошенников. Полезные советы по безопасности

Дабы максимально оградить себя от посягательств злоумышленников, при работе в Интернете следует соблюдать меры предосторожности и правила, которые перечислены ниже.

♦ Прежде чем выходить в Интернет, установите на компьютер хорошую антивирусную программу. Следите за тем, чтобы антивирусные базы все время были актуальными, и помните, что в мире ежечасно появляется несколько новых вирусов.

♦ Никогда не храните логины, пароли, пин-коды, номера кредитных карт и прочие конфиденциальные сведения в открытом виде – например, в обычном текстовом файле, или на бумажке, прикрепленной к монитору. Как показывает практика, множество афер совершается благодаря тому, что беспечная жертва своевременно не позаботилась о хранении секретных данных в надежном месте.

♦ Если вы подключаетесь к Интернету через телефонную линию, никогда не выключайте динамик модема. Это позволит сразу распознать попытки интернет-мошенников несанкционированно подключить ваш компьютер к тому или иному удаленному веб-ресурсу путем набора заданного телефонного номера (часто это практикуют распространители порнографических сайтов и услуг подобной направленности).

♦ Если вы все же хотите хранить все конфиденциальные данные в одном файле – заархивируйте этот файл и защитите архив надежным паролем (минимум из 16 символов). Рекомендуется использовать для этого архиватор WinRAR – как показывает практика, расшифровать такой пароль практически нереально.

♦ Если вы услышали, что модем начал самопроизвольно набирать какой-то номер без вашего участия – срочно отключитесь от Интернета путем физического отсоединения кабеля. Затем просканируйте компьютер специальной программой категории Antispyware (антишпионским приложением) – очень может быть, что в компьютер тайно внедрен шпионский модуль автоматического дозвона. В конечном итоге это чревато получением астрономических счетов от телефонной компании.

♦ Не доверяйте посторонним свои учетные данные, а также не предоставляйте право пользования своими электронными кошельками, управления банковскими счетами через Интернет, и т. п. К сожалению, нередко мошенниками становятся именно те, кому вы больше всего доверяете. Кроме этого, даже если доверенное лицо является кристально честным человеком, ваши конфиденциальные данные у него могут просто похитить.

♦ Будьте максимально бдительны и осторожны при посещении неизвестных страниц в Интернете. Сегодня широко распространены шпионы и вирусы, для заражения которыми достаточно просто зайти на определенную веб-страницу.

♦ Электронную корреспонденцию, поступившую от неизвестных и сомнительных отправителей, перед открытием обязательно проверяйте надежной антивирусной программой (с актуальными базами). Несоблюдение этого правила может привести к тому, что ваш компьютер быстро превратится в «шпионское гнездо».

♦ После скачивания из Интернета файлов, архивов и т. п. надо сразу же проверить их антивирусной программой, и только после этого запускать на выполнение, распаковывать и т. д. Помните, что многие вредоносные программы распространяются в виде исполняемых файлов либо архивов.

♦ Если вы пользуетесь операционной системой Windows – регулярно проверяйте ее на предмет безопасности. В частности – своевременно скачивайте с сайта Microsoft и устанавливайте на свой компьютер все последние обновления, касающиеся безопасности (так называемые «заплатки»).

♦ Никогда не отвечайте на запросы и письма, в которых содержится просьба прислать ваши секретные данные (логин, пароль, пин-код и т. п.) по указанному адресу. Этот нехитрый способ (разновидность так называемой «социальной инженерии») позволяет злоумышленникам получить чужие логины, пароли, пин-коды кредитных карт, и иные конфиденциальные сведения.

♦ Если при посещении различных ресурсов в Интернете (форумы, страницы регистрации, и т. д.) требуется оставить о себе некоторые данные, то они должны содержать минимум сведений. В частности, никогда и никому не сообщайте свои паспортные данные, домашний адрес, различные пароли и т. п. Несмотря на то, что владельцы и руководители многих Интернет-ресурсов гарантируют полную конфиденциальность, не будьте наивными: если кому-то надо получить эту информацию, он ее получит, и вполне может использовать для шантажа, вымогательства и т. п.

♦ По окончании работы в Интернете обязательно отсоединяйте кабель от линии соединения с Интернетом. Помните, что в противном случае ваш компьютер будет уязвимым даже в выключенном состоянии.

Помимо перечисленных правил безопасности, при работе в Интернете руководствуйтесь нормами и принципами, которые диктуется здравым смыслом и элементарной осторожностью.

1.7. Что делать и куда обращаться, если вы стали жертвой мошенников?

1. РОСПОТРЕБНАДЗОР www.rospotrebnadzor.ru/freedback/new.php

В эту Службу можно обратиться с заявлением или жалобой на действия организаций, оказывающих финансовые услуги.

2. БАНК РОССИИ www.cbr.ru/Reception/

При Банке России действует Служба по защите прав потребителей финансовых услуг и миноритарных акционеров.

3. АГЕНСТВО ПО СТРАХОВАНИЮ ВКЛАДОВ
   www.asv.org.ru/contacts Агентство осуществляет ликвидацию и банкротство банков, выплачивает страховые возмещения по вкладам.
4. ФЕДЕРАЛЬНАЯ АНТИМОНОПОЛЬНАЯ СЛУЖБА
   www.fas.gov.ru/contacts/contact-info
   Пресекает недобросовестную рекламу и обман потребителей.
5. ФИНАНСОВЫЙ ОМБУДСМЕН www.arb.ru/b2c/abuse

Рассматривает обращения и жалобы граждан по факту ненадежного оказания финансовых услуг.

6. СУД

При споре с организациями, оказывающими финансовые услуги, можно обратиться в суд по месту жительства.

С февраля 1999 г., когда Министерство юстиции учредило Программу борьбы с мошенничеством в Интернете, федеральное правительство еще более активно стало сочетать уголовное преследование с координированным анализом и расследованием в рамках глобальной борьбы с мошенничеством в Интернете.

Заключение

Мошеннический обман весьма разнообразен по содержанию в своих конкретных проявлениях: Обман может быть устным и письменным, он может заключаться в фальсификации предмета сделки, в применении шулерских приемов при игре в карты или «в наперсток», в использовании при расчете фальсифицированных предметов расплаты. Обман может совершаться путем использования подложных документов. Он может быть связан с характеристикой предметов при совершении различных сделок (их ценности, количества и качества, самого факта их наличия и т.д.), введением в заблуждение относительно якобы имеющихся оснований для передачи имущества, различных событий и действий. Исходя из этого, можно сделать вывод, что, находясь в Интернете, нужно быть бдительным, осторожным, меньше доверять тому, что пишут вам или на сайтах, которые вы посещаете. Мошенничество может быть совершено только с прямым умыслом. Обязательный признак субъективной стороны–корыстная цель.

Изучив материал по теме моей работы, я смогла прийти к выводу что. Финансовое мошенничество - довольно опасное и частое явление, способное проявляться в различных его формах. И даже несмотря на то, что рассматриваемая проблема кажется от нас далёкой, необходимо быть с ней знакомым и знать, как с ней бороться. Она может коснуться любого из нас, каким бы осторожным человек ни был.

В ходе защиты проекта были достигнуты его цель и задачи:

1. Аудитория была ознакомлена с понятием финансового мошенничества
2. Понятие было раскрыто и пояснено
3. Были изучены виды и особенности финансового мошенничества
4. Были найдены и описаны пути минимизации рисков

Список литературы и источников

1. Алексей Горяев, Валерий Чумаченко - «Финансовая грамота» - Юнайтед Пресс, 2012. https://finagram.com/finshop/finbooks/

2. Безопасность детей в Сети Интернет ©2006 Корпорация Microsoft

3. http://www.detionline.ru/lying.htm

4. http://rumetrika.rambler.ru/review/

5. http://www.oszone.net/4479/News_Microsoft

6. http://www.greenmama.ru

7. Дэниел Голди, Гордон Мюррей-«Инвестиционный ответ»-Альпина Паблишер, 2011. https://finagram.com/finshop/finbooks/

Приложения

Вместе с научным руководителем, мы составили задачи по финансовой грамотности, которые относятся к теме нашей научно-исследовательской работы, которые помогут выбрать верное решение в той или иной ситуации. Подобные задачи являются одним из заданий в ОГЭ по «Обществознанию» для 9 класса. (Приложение 1)

Кроме этого была напечатана методичка с советами «Как не попасться на удочку мошенников» (Приложение 2)

Приложение 1

Задачи по финансовой грамотности

Задача №1

Андрей решил взять кредит в банке для покупки автомобиля. Он изучил предложения по кредитам нескольких банков, остановил свой выбор на предложении с наиболее низкими процентами по кредиту. На какие другие условия кредитования стоит обратить внимание Андрею? Как ему следует поступить, чтобы выплатить кредит в срок?

Ответ:

1) Следует обратить внимание на расчёт графика погашения кредита, размер дополнительных расходов;

2) Следует строго придерживаться графика платежей, избегая возможных задолженностей по выплатам и пеней.

Задача №2

Ольге на телефон пришло сообщение о поступлении 5000 рублей на её счёт в банке, затем раздался телефонный звонок, и звонивший потребовал вернуть средства, якобы переведенные по ошибке, убеждая Ольгу назвать номер банковской карты и другую информацию по счёту.

В чём состоит опасность данной ситуации для личных финансов Ольги? Как ей правильно поступить в данной ситуации?

Ответ:

1) Опасность заключается в том, что посылают смс и звонят одни и те же мошенники, которые надеются обескуражить человека и получить возможность вывести деньги с его счёта;

2) Необходимо проверить состояние своего счёта, например, посредством мобильного банка, и ни в коем случае по телефону не сообщать никаких данных.

Задача №3

Сидору П. в наследство от бабушки досталась половина квартиры в соседнем городе. Он продал эту часть второму наследнику за 1,3 млн руб. Доход был неожиданным, и Сидор не хотел сгоряча принимать решение, как лучше распорядиться деньгами, а решил пока положить их в банк под проценты. Его друг Арнольд предложил ему разместить деньги в недавно появившейся организации «К.», которая обещала через месяц доход в три раза выше годового дохода по банковскому депозиту. Какой выбор следует сделать Сидору?

Ответ:

1) Сидору стоит разместить деньги в банке под процент.

2) Обоснование: вклад в банке застрахован, следовательно даже в случае банкротства банка, деньги Сидор сохранит; проценты по вкладу защитят деньги от обесценивания; вариант предложенный Арнольдом содержит признаки финансовой пирамиды, участие в которой может лишить Сидора денег.

Задача №4

Семену пришло сообщение в социальной сети от его друга Петра: «Привет, Семен! Не выручишь деньгами до вторника? А то баланс на телефоне отрицательный, а срочно надо связаться с родителями. Скинь 500 рублей на номер ***». В чём состоит опасность данной ситуации

для личных финансов Семена? Как ему правильно поступить в данной ситуации?

Ответ:

1) Скорее всего это мошенники, которые взломали аккаунт Петра в социальной сети и рассылают сообщения от его имени с целью наживы.

2) Ни в коем случае не отсылать деньги на указанный номер; обратиться на «горячую линию» для клиентов и/или в службу социальной сети; позвонить Петру и сообщить ему о полученном сообщении.

Задача №5

Совершеннолетней Анне Ф. пришло СМС−сообщение со следующим текстом: Поздравляем! Вы выиграли новый автомобиль BMW, для получения приза свяжитесь с нами по номеру ***. Позвонив по телефону, Анна узнала, что ей необходимо уплатить небольшую сумму в качестве таможенной пошлины за растаможивание автомобиля и получила номер карты, на которую нужна, перевести сумму. В чём состоит опасность данной ситуации для личных финансов Анны Ф.? Как ей правильно поступить в данной ситуации?

Ответ:

1) защита Отечества;

2) два объяснения, допустим:

— это обеспечивает возможность другим гражданам реализовывать свои права, закрепленные законом;

— это позволит обществу и государству планомерно развиваться, предотвратит рост социального напряжения и конфликты.

Задача №6

Петр учится в 10-ом классе. Он хочет купить новый смартфон определенной модели и марки, но у него не хватает накопленных денег. Тогда он начинает искать данную модель смартфона в интернете. На одном из сайтов Петр нашел данную модель со стоимостью в три раза

ниже, чем в магазине. Единственным условиям, которое насторожило Петра, было требование внести 100% предоплаты на электронный кошелек. В чём состоит опасность данной ситуации для личных финансов Петра? Как ему правильно поступить в данной ситуации?

Ответ:

1) Скорее всего это мошенники, о чем свидетельствует необъяснимо низкая цена; после внесения предоплаты смартфон либо не придет к получателю, либо придет его некачественная подделка, а деньги обратно будет не получить, так как магазин исчезнет.
2) Ни в коем случае не покупать в интернет−магазинах с подозрительно низкими ценами, пользоваться услугами проверенных фирм.

Задача №7

Листая ленту в социальной сети Аркадий увидел просьбу о помощи ребенку, которому требуется срочная операция, иначе он умрет. В обращении был указан номер карты, на которую можно перечислить материальную помощь.

В чём состоит опасность данной ситуации для личных финансов Аркадия? Как ему правильно поступить в данной ситуации, если он хочет заняться благотворительностью?

Ответ:

1) Скорее всего это мошенники, которые используя ненастоящие фотографии и данные пытаются выманить у сердобольных граждан денежные средства.

2) Необходимо обратиться в известный благотворительный фонд, которому можно доверять; можно попытаться связаться с семьей данного ребенка и посетив ее выяснить, на самом деле им требуется помощь или это обман.

Задача №8

Совершеннолетнему Оскару пришло SMS-сообщение с короткого номера: «Уважаемый клиент! Ваша карта заблокирована, перезвоните по телефону ***. Для оперативности приготовьте Ваши паспортные данные и следующие данные по Вашей карте: № и PIN-код. Наш оператор решит данную проблему после вашей идентификации».

В чём состоит опасность данной ситуации для личных финансов Оскара? Как ему правильно поступить в данной ситуации?

Ответ:

1) Скорее всего это мошенники, которые планировали получить конфиденциальную информацию и снять со счёта все деньги.

2) Ни в коем случае не перезванивать и не сообщать номер своего банковского счёта/карты и PIN-код; обратиться на «горячую линию» для клиентов и/или в службу безопасности банка.

Задача №9

Ольге на телефон пришло сообщение о поступлении 5000 рублей на её счёт в банке, затем раздался телефонный звонок, и звонивший потребовал вернуть средства, якобы переведенные по ошибке, убеждая Ольгу назвать номер банковской карты и другую информацию по счёту. В чём состоит опасность данной ситуации для личных финансов Ольги? Как ей правильно поступить в данной ситуации?

Ответ:

1) Опасность заключается в том, что посылают смс и звонят одни и те же мошенники, которые надеются обескуражить человека и получить возможность вывести деньги с его счёта;

2) Необходимо проверить состояние своего счёта, например, посредством мобильного банка, и ни в коем случае по телефону не сообщать никаких данных.

Задача №10

Шестнадцатилетняя Екатерина искала работу, график которой можно было бы совместить с учёбой в колледже. В Интернете она нашла предложение следующего содержания: «Работа в удобное время. Набор текста. 1 лист – 100 рублей. Количество листов зависит только от вашего желания. Для получения первого заказа вы должны перечислить 500 рублей на электронный кошелёк работодателя! Торопитесь! Осталось 8 вакансий!» Оцените ситуацию с точки зрения достижения цели Екатерины. Как ей правильно поступить в данной ситуации?

Ответ:

1) Скорее всего Екатерина не найдёт работу. Объявление дали мошенники: они предлагают большие деньги при минимальном вложении труда и при устройстве на работу деньги платит работодатель работнику, а не наоборот;

2) Ответ на второй вопрос, например: не переводить деньги, уточнить информацию о том, сколько стоит в среднем выполнение данного вида работы.

Приложение 2

Методическое пособие для людей всех возрастов.

Финансовое мошенничество-это глобальная проблема?

Во всем мире отмечен резкий рост случаев мошенничества. Сколько ни предупреждает полиция, сколько ни рассказывают СМИ о том, как простодушные граждане попадаются на удочку финансовых мошенников, год за годом преступники выуживают у людей сотни тысяч, если не миллионы денежных средств. Проблема не только в легковерии, но и в том, что аферисты придумывают все новые и новые формы обмана. Тем самым денежные средства не совершают свой круговорот, и поэтому страдает большая часть экономики мира.

Определение финансового мошенничества

Финансовое мошенничество - совершение противоправных действий в сфере денежного обращения путем обмана, злоупотребления доверием и других манипуляций с целью незаконного обогащения.

Виды мошенничества:

Телефонное мошенничество. Для обмана жертвы через телефон используются смс-рассылка или звонки с телефонного номера. Мошенники всем способами будут пытаться узнать (номер карты, срок действия карты, CVC/CVV код)

Финансовое мошенничество. Происходит в основном у банкомата, Данные карты могут сканировать с помощью скиммера, а пин-код заполучить с помощью незаметной видеокамеры или накладки на клавиатуру

Кибермошенничество. Приходит СМС или письмо «от банка» со ссылкой, просьбой перезвонить или уведомление о крупном выигрыше. Или звонят «из банка» и просят отправить личные данные. Или пишут в социальных сетях от имени родственников или друзей, которые попали в беду, и просят перевести деньги на неизвестных счет.

Черные кредиторы. Если разрешения у компании (или лицензии у банка) нет, а она все равно привлекает клиентов, выдает себя за лицензированную и кредитует потребителей, то это нелегальный, или черный, кредитор.

Чаще всего жертвами мошенничества становятся:

- Женщины чаще всего становятся жертвами мошенников. Отмечено, что женщины менее внимательны. Тем самым мошенникам легче добраться до жертвы.
- Вторая группа жертв аферистов - это "школьники, студенты, лица с особенностями социальной адаптации". Эти граждане доверчивые, расточительные, импульсивные, склонные к риску, у них - "противоречивая самоидентификация"
- Третью группу назвали "бюджетораспорядителями семей с невысоким уровнем дохода и высокой финансовой нагрузкой". Это целеустремленные и ответственные люди, которые высоко ценят семейные и дружеские связи, ответственные.
- Четвертая группа - "домохозяйки" - уступчивые, доверчивые.
- Пятая группа - "серебряный возраст", в нее входят россияне старше 60 лет.

Чтобы никогда не попасться к телефонным мошенникам нужно:

- Не отвечать на подозрительные письма
- Не сообщать данные карты никому, даже сотруднику банка

Что делать, если вас всё-таки обманули телефонные мошенники:

- Срочно позвоните в банк
- Попросите заблокировать карту
- Обратитесь в банк с паспортом
- Запросите выписку со счёта
- Напишите заявление о несогласии с операцией
- Обратитесь в полицию

Как не попасться к финансовым мошенникам?

- Осматривайте картоприёмник и клавиатуру, на них не должно быть посторонних предметов
- Набирая пин-код, прикрывайте клавиатуру рукой
- Не пользуйтесь банкоматами неизвестных банков
- Не упускайте карту из виду даже на 5 секунд

Кибермошенничество. Как не попасться?!

- Не переходите по неизвестным ссылкам, не перезванивайте на сомнительные номера.
- Никому не сообщайте персональные данные, тем более пароли и коды.
- Не храните данные карт на компьютере или в смартфоне.
- Проверяйте информацию. Если вам звонят и сообщают что-то о вашем счете (по ошибке списали или зачисли деньги), не следуйте никаким инструкциям и срочно сами звоните в банк.
- Установите на компьютере антивирус.

Как распознать черного кредитора?

- Проверьте, есть ли компания в реестре на сайте Банка России.
- Если компании нет в Справочнике по кредитным организациям или в Справочнике участников финансового рынка на сайте Банка России — это не легальный кредитор.

Как черные кредиторы обманывают клиентов?

- Сомнительные бумаги
- Предоплата за кредит
- Использование данных

Как не попасть к черным кредиторам? 4 простых правила

- Осматривайте картоприёмник и клавиатуру, на них не должно быть посторонних предметов
- Набирая пин-код, прикрывайте клавиатуру рукой
- Не пользуйтесь банкоматами неизвестных банков
- Не упускайте карту из виду даже на 5 секунд

Ещё несколько советов, которые помогут избежать финансового обмана:

- Подключите услугу смс-оповещения по операциям с вашей банковской карты
- Заведите несколько банковских карт
- Установите лимит на съём денег и оплату по карте
- Не храните пин-код вместе с картой