ФИНАНСЫ

ЦЕНТР
ЗАЩИТЫ ПРАВ ГРАЖДАН

справедливо-центр.рф
8-800-755-55-77

КАК ОБЕЗОПАСИТЬ СЕБЯ И БЛИЗКИХ ОТ МОШЕННИКОВ
Часть 2

«Липовое» повышение пенсий

Вирусные программы для дистанционных работников

Вымогательство в банках и по электронной почте

Опасные лотереи и многое другое

ПРОГРАММА ПРАВОВОГО ПРОСВЕЩЕНИЯ ГРАЖДАН

ЦЕНТР ЗАЩИТЫ ПРАВ ГРАЖДАН
справедливо-центр.рф
8-800-755-55-77

КАК ОБЕЗОПАСИТЬ СЕБЯ И БЛИЗКИХ ОТ МОШЕННИКОВ Часть 2

«Липовое» повышение пенсий

Вирусные программы для дистанционных работников

Вымогательство в банках и по электронной почте

Опасные лотереи и многое другое

СОДЕРЖАНИЕ

Каждый второй россиянин хотя бы однажды становился жертвой мошенников. Беда в том, что зачастую люди отдают им деньги по собственной воле.

Но современные злоумышленники научились не просто отбирать наличность или навязывать кредит. Способы становятся день ото дня все изощреннее.

Если раньше мошенник представлялся сотрудником банка, теперь он уже шлет письмо от имени Центробанка.

Не получилось навязать втридорога водосчетчик – вам под угрозой опасности взрыва продадут газоанализатор и дымоуловитель.

Мошенники не гнушаются отбирать последнее у пенсионеров. И сегодня обрабатывают пожилых людей на теме повышения пенсий.

Не отстают и вполне легальные организации: и вот уже банк пытается продать услугу, которая изначально является бес-

платной для клиента. Пандемия тоже внесла свою лепту. Липовые справки о вакцинации, попытка влезть в компьютеры дистанционных работников и многое другое.

Ежегодный ущерб россиян от действий мошенников составляет 500 млрд рублей! Потеряли вы в результате обмана 100 рублей или 100 тысяч рублей – итог один: отчаяние, негодование, злость на себя за глупость, желание вернуть свое и наказать обидчика.

Для того чтобы минимизировать риск быть обманутым, обезопасить себя и близких от потерь, Центр защиты прав граждан продолжает разрабатывать инструкции о том, как защититься от самых болезненных видов мошенничества.

В первом кейсе **«Как обезопасить себя и своих близких от мошенников»** мы подробно описали финансовые махинации при денежных переводах и обманные схемы при покупке и продаже товаров. Навязывание псевдомедицинских процедур, приобретение «чудо-посуды» и предложение от всемогущих экстрасенсов и магов, которым порой так трудно отказать. А также поговорили о том, как обманывают собственников организации, занимающиеся установкой водосчетчиков и пластиковых окон.

В этой инструкции мы рассмотрим еще десять не менее опасных способов оставить человека без денег.

Расскажем, на что стоит обратить внимание, чтобы не угодить на крючок.

Дадим советы, как действовать при контакте со злоумышленником.

Подскажем, как уберечь самых доверчивых и незащищенных людей – родителей, дедушек и бабушек, которые чаще всего становятся жертвами аферистов.

Как говорится, предупрежден – значит вооружен!

Полезного чтения.

МОШЕННИЧЕСТВО №1: ПРОДАЖА ПОДДЕЛЬНЫХ СЕРТИФИКАТОВ О COVID-ВАКЦИНАЦИИ

Это новый вид мошенничества, который возник в период пандемии COVID-19. Хотя сама схема по сути своей стара как мир и представляет из себя простую продажу поддельного документа. В данном случае человеку предлагается приобрести якобы настоящий сертификат вакцинированного от COVID-19.

А поскольку вакцинация с каждым месяцем набирает обороты по всей стране, увеличивается и спрос на приобретение «липовой» справки.

На уловку попадаются люди, которые по тем или иным причинам не хотят вакцинироваться. В то время как многие работодатели или туроператоры требуют от человека привиться и предъявить соответствующий сертификат вакцинированного от ковида. Чем и пользуются недобросовестные любители легкой наживы.

Это могут быть как организации, так и просто физлица, оказывающие подобные услуги. Суть от этого не меняется. Человеку предлагается справка якобы с настоящими печатями, ничем не отличающаяся от оригинала, с подписями «настоящих медиков».

Стоимость справки варьируется от 1,5 до 3 тысяч рублей. А в качестве доказательства вам даже любезно сбросят пару фотографий, показывающих, как этот сертификат выглядит.

Если жертва клюнула, сценариев может быть два. Либо человек заплатит и все же получит документ, который на самом деле наметанный глаз легко отличит от оригинала. Либо жертва вообще не получит ничего: отправит деньги мошенникам, заплатив за воздух.

Подобные действия грозят человеку не только потраченными деньгами и нервами. Напомним, что за приобретение и использование заведомо поддельного официального документа в России установлена уголовная ответственность. Так что по своей неосторожности или глупости жертва в дальнейшем может получить тюремный срок до одного года или как минимум будет отправлена на общественные работы.

КАК ЭТОГО ИЗБЕЖАТЬ

Мы настоятельно не рекомендуем нарушать закон, покупая поддельные справки и документы.

Сейчас, за исключением ряда профессий и категорий граждан, процедура вакцинации от ковида является добровольной.

Если не намерены прививаться или хотите сделать это позже, решение за вами.

МОШЕННИЧЕСТВО №2: ОБМАН СОИСКАТЕЛЕЙ РАБОТЫ И УСТАНОВКА ВИРУСНЫХ ПРИЛОЖЕНИЙ

Пандемия коронавируса и массовый переход организаций на удаленную работу изменили мышление не только обычных людей, но и мошенников.

Так, все популярнее становится новый вид цифрового

мошенничества, жертвами которого становятся соискатели работы (в основном удаленной).

Схема здесь следующая.

Желающие нажиться на людях нечестным путем с определенным набором компьютерных навыков находят на порталах с вакансиями резюме людей, которые ищут работу и, естественно, оставляют в анкете свои контактные данные. После чего мошенники под видом потенциальных работодателей связываются с жертвой и просят установить на свой телефон одно или несколько приложений – якобы для проверки профессиональных навыков или прохождения онлайн-собеседования и т. д.

Опасность в том, что приложение содержит встроенный вирус, который жертва собственноручно запускает в свой телефон/компьютер. Примечательно, что зараженные приложения скачиваются из официальных источников вроде магазина Google Play. Что изначально не вызывает подозрений у жертвы. А тем временем вирус из установленного приложения проникает в устройство и получает доступ к конфиденциальной информации. Включая логины и пароли от входа в почту, аккаунты в социальных сетях, данные банковских карт, а иногда и личные коды клиента банка.

Стоит ли говорить, чем опасно завладение такими данными третьими лицами? Результатом станет опустошение банковского счета, перенастройка аккаунта в соцсетях или даже шпионаж.

КАК ЭТОГО ИЗБЕЖАТЬ

Во-первых, следует тщательно проверять информацию об организации, которая предложила вам работу. Сейчас благодаря интернету вы можете досконально проверить работодателя. Это может быть информация о постановке на учет, отзывы сотрудников, юридический адрес, судебные прецеденты. Если это фирма-однодневка, вряд ли вы найдете о ней много подробно-

стей. Или же найдете негативные отзывы тех, кто стал жертвой махинаций. В этом случае вежливо откажитесь от предложения и занимайтесь поисками работы дальше.

Во-вторых, помните, что даже онлайн-собеседования обычно проводятся в популярных приложениях. К примеру, Skype или Zoom. И даже если вы ранее не пользовались таким, его можно скачать на официальных сайтах. Работодатель не будет просить загрузить на ваше устройство какие-либо иные приложения для прохождения онлайн-интервью. В редких случаях (обычно в организациях, представляющих органы власти) компания может иметь свой сервис для прохождения удаленных собеседований. Но, как правило, представитель работодателя направит вам ссылку на подключение к онлайн-конференции. И не более того.

В-третьих, не забывайте про пользу антивирусных программ. Причем как на персональных компьютерах, так и на смартфонах и планшетах. Помните, что хороший, пусть и платный антивирус, не только может обезопасить вас в подобных случаях, но и защитит от различных вирусов во время интернет-серфинга.

В любом случае не покупайтесь на работу мечты и обещанные золотые горы, если первым делом вас просят что-то закачать или установить на своем оборудовании. Потратьте время и убедитесь, что вакансия существует и компания такая тоже успешно работает на рынке.

МОШЕННИЧЕСТВО №3: ОБМАН ПЕНСИОНЕРОВ И ФЕЙКОВОЕ ПОВЫШЕНИЕ ПЕНСИЙ

Пожалуй, сегодня это один из самых циничных и распространенных видов мошенничества, касающийся пенсионеров.

Люди преклонного возраста живут на скромные пенсии и рады любой лишней копеечке. Стоит ли удивляться, что, уз-

нав, что пенсию можно повысить, наши пенсионеры соглашаются на условия мошенников?

А у тех – целый ассортимент обманных схем на эту тему.

Это может быть письмо в почтовый ящик (или электронное письмо) якобы от юридической организации или даже представительства Пенсионного фонда РФ. То есть заочный метод.

Может быть и прямой контакт, когда на пороге квартиры пенсионера (чаще всего одинокого) появляется человек якобы из соцзащиты, Пенсионного фонда или юридической фирмы.

Причем мошенники заранее точно знают, к кому они обращаются. Владеют персональными данными жертвы. Знают возраст и даже сегодняшний размер пенсии.

Уловка в том, что пенсионеру предлагают довериться организации, которая сможет добиться от властей увеличения размера пенсии.

Где-то убеждают, что вышел «новый закон». Где-то просто уверяют, что у Вас, Мария Ивановна, недосчитан трудовой стаж.

Разумеется, когда звучит сумма в 3–7 тысяч рублей ежемесячно к пенсии, у пожилых людей в глазах загорается огонек надежды: вдруг действительно получится – и я буду жить лучше?

Чтобы это «вдруг» настало, пенсионеру предлагают заплатить за услуги юриста (адвоката).

Размер гонорара подбирается с учетом качества жизни в регионе и состоятельности пенсионера. Где-то услуга оценивается от 40 до 60 тысяч. В республиканских и областных столицах за содействие попросят 100 тысяч. В Москве и Санкт-Петербурге ставка доходит до 300 тысяч рублей. Зафиксирован случай, ког-

да пенсионер отдал полмиллиона в обмен на обещание добавить к его пенсии в пять раз больше.

Чтобы все выглядело легально, пенсионеру предлагают проехать в заранее снятый мошенниками офис и заключить договор. В офис с фирменной табличкой, где снуют люди в костюмах, звонят телефоны и выглядит все вполне официально.

В офисе пожилому человеку подсовывают договор с кучей юридических терминов вроде «подбор специалистов», «представление интересов в суде», «перерасчет пенсионных выплат» и прочее.

Но главное – в нем жирно выделена повышенная сумма, которую ежемесячно человек в скором времени якобы начнет получать. Обычно повышенную пенсию обещают уже через один-два месяца после заключения договора.

Итак, договор подписан, услуга оплачена, но по истечении обещанного срока размер пенсии почему-то не увеличивается. Ни через два месяца, ни через полгода. Пенсионер начинает звонить «адвокату», но телефон выключен. Едет в офис, но там уже ни таблички, ни людей в деловых костюмах.

К сожалению, таких примеров становится все больше.

Есть случаи, когда особо наглые мошенники под видом другой юридической фирмы повторно выходят на того же пенсионера. Внушают, дескать, Мария Ивановна, вы с тали жертвой аферистов. Мы поможем и аферистов поймать, и пенсию повысить, но только надо заключить договор. Все повторяется, и пенсионер во второй раз остается у разбитого корыта.

КАК ЭТОГО ИЗБЕЖАТЬ

Необходимо помнить, что пенсионными делами российских пенсионеров заведует Пенсионный фонд России. А значит, всей информацией о размере, ежегодной индексации, учете льгот и стажа, дополнительных выплатах владеет только ПФР.

Да, действительно, в силу технических ошибок при расчете пенсии может быть не учтен нестраховой период, часть стажа и пр. Это влияет на размер пенсии. Но вопросы урегулирования таких недоразумений решаются только в официальных представительствах ПФР. Проверка правильности пенсионных начислений делается по заявлению пенсионера.

Если вы не знаете, как проверить размер своей пенсии и составить заявление в Пенсионный фонд, обратитесь за консультацией в Центры защиты прав граждан. Разобраться с правильностью начисления пенсии специалисты Центров помогут абсолютно БЕСПЛАТНО.

Что касается писем о «новом законе», гарантирующем надбавки, или появлении на пороге квартиры «представителя ПФР» – будьте бдительны. Если у вас просят деньги за помощь в повышении размера пенсии – это обман.

Не стесняйтесь задавать неудобные вопросы «представителю ПФР». Потребуйте контакты руководителя, подтверждений на законные основания. Зачастую скрупулезное изучение информации отпугивает мошенников, ведь жертва тем самым может без труда вывести их на чистую воду еще до подписания договора и передачи денег.

Если же дело дошло до выезда в офис, ни в коем случае ничего не подписывайте и уж тем более не отдавайте никому деньги. Прочитайте договор. Обычно мошенники оперируют в них общими словами и фразами, а также «резиновыми формулировками». Которые не только не несут в себе конкретики, но и в будущем позволяют фирмам-однодневкам уходить от уголовного преследования.

Кроме того, зачастую уплачиваемые деньги несоразмерны возможной выгоде.

Защититься от подобного рода афер могут помочь дети и внуки пенсионеров. Молодое поколение априори более подковано в таких вопросах. Присматривайте за вашими родителями, бабушками и дедушками. Не поленитесь лишний раз провести с ними беседу и рассказать о том, как их могут обмануть подобные «специалисты».

МОШЕННИЧЕСТВО №4: ОБМАН ЛЮДЕЙ В БАНКАХ ПУТЕМ НАВЯЗЫВАНИЯ КРЕДИТОВ И ДОПУСЛУГ

Сразу отметим: с правовой точки зрения любая оказываемая банком или микрофинансовой организацией услуга, скрепленная с заемщиком договором, мошенничеством не является.

Но если учесть, при каких обстоятельствах зачастую эти договоры заключаются, и добавить человеческий фактор, то этот способ нажиться на людях (и особенно на пенсионерах) вполне можно отнести к разновидности мошенничества.

Некоторые банки и МФО обманывали (вводили в заблуждение) своих клиентов и раньше. Но в последнее время, из-за пандемии коронавируса, количество такого рода обманов выросло в разы.

Этому способствовали два фактора.

Во-первых, пандемия лишила многих людей работы и, следовательно, заработка. У пострадавших появилась острая потребность в деньгах, в том числе и в кредитных.

Во-вторых, из-за введенных ограничений в связи с режимом повышенной готовности поток клиентов в банках вынужденно

сократился. Многие работники кредитно-финансовых организаций остались без премий и надбавок. Ведь премии зачастую зависят от количества проданных клиенту услуг. Поэтому, как только двери кредитных организаций снова распахнулись, «обрабатывать» людей (особенно пенсионеров) менеджеры стали усерднее вдвойне.

В результате клиент сегодня может угодить в самый настоящий кредитный капкан. Достаточно согласиться с навязанными и совершенно ненужными дополнительно оплачиваемыми услугами.

Так, сотрудники банков не стесняются «садиться людям на уши» и предлагать «особо выгодные» условия по кредиту. Которые на самом деле таковыми не являются. Задача менеджера – выдать человеку кредит под как можно более выгодный для финансовой организации процент. А если процент фиксированный, то навязать как можно больший кредит, чтобы и процентов по нему «накапало» больше.

При этом финансовые возможности клиента или его тяжелая жизненная ситуация банк абсолютно не интересуют. Все равно рано или поздно клиент вернет все. Не добровольно, так через суд.

Ненужные дополнительные услуги – еще один бич клиента любого, даже самого крупного банка.

К примеру, клиент кредитуется на 500 тысяч рублей, а дополнительно навязанная страховка обходится ему еще в 100 тысяч.

Незначительные суммы – это когда банк навязывает дополнительные сервисы в виде подключения услуги СМС-информирования по карте за 99 рублей в месяц. И это несмотря на то, что уведомления в банковском приложении будут приходить бесплатно на протяжении всего периода кредитования.

Чаще всего жертвами подобных допуслуг становятся опять же возрастные клиенты, которые привыкли доверять мнению профессионалов.

КАК ЭТОГО ИЗБЕЖАТЬ

Главный совет – прежде чем взять кредит, нужно хорошо обдумать данное решение. В самом механизме кредитования ничего плохого и нет, но следует трезво оценивать свои возможности его вернуть. Причем с приличными процентами.

Если же иного выхода нет, следует обращаться только в крупные и надежные банки. Поскольку в любом случае таким финансовым организациям небезразлична собственная репутация. И при возникновении спорных вопросов или непредвиденных обстоятельств банк может пойти навстречу клиенту. Мы не рекомендуем обращаться за займом в микрофинансовые организации. Да, деньги там выдают быстро, но проценты будут в десятки (а то и сотни раз) выше банковских.

Если банк выбран, а программа кредитования вам подходит, внимательно изучите кредитный договор перед подписанием.

Любой, даже самый уважаемый банк все равно старается извлечь из сделки выгоду. И нередко в договоре есть «подводные камни» или пояснения мелким шрифтом, которые зачастую сводят всю выгоду по кредиту на нет.

Если подписали договор, а потом прочитали его и передумали, помните: у кредитов тоже существует так называемый период охлаждения.

В течение 14 дней клиент имеет право вернуть кредит банку (это федеральный закон, но все же проверяйте, чтобы этот пункт тоже значился в договоре).

Важно знать, что период охлаждения не исключает оплату накапавших процентов. То есть проценты за фактический период нахождения у вас на руках выданных средств выплатить придется.

Что касается дополнительных услуг, помните, что здесь вы можете отказать банку в предложении (а иногда даже требовании) оформить ту или иную услугу.

Если речь идет о страховке по кредиту, оформлять страховой полис по закону не требуется. Да, банк имеет право отказать вам в кредите без оформления полиса. Но если это крупный банк, такое вряд ли произойдет.

Любые другие дополнительные услуги (как более крупные, так и более мелкие вроде СМС-информирования) вы в любом случае сможете получить всегда. Причем многие из них можно оформить онлайн, не посещая отделение банка. Поэтому, как бы это грубо ни звучало, отгоняйте консультантов, пытающихся навязать вам такие услуги, как мух.

Если вы не можете самостоятельно разобраться, законно ли банк требует от вас оформить страховку или оплатить подключение к сервисам, обратитесь за консультацией в Центр защиты прав граждан. Специалисты помогут вам отказаться от навязанных услуг и вернуть переплату. Юридическая помощь в Центрах оказывается БЕСПЛАТНО.

МОШЕННИЧЕСТВО №5: МАССОВЫЕ ОБМАНЫ ГРАЖДАН ПОД ВИДОМ ЦЕНТРОБАНКА РФ

Сразу три новые схемы мошенничества, но все связанные с упоминанием Центробанка РФ, продолжают набирать популярность на всей территории России.

Общее в них то, что мошенники выходят на жертву (звонят или связываются через социальные сети) и представляются либо сотрудниками Центрального банка России, либо сотрудниками правоохранительных органов, действующих от ЦБ.

Но обо всем по порядку.

ПЕРВЫЙ СПОСОБ возник на фоне пандемии коронавируса – это якобы выплаты от государства на поддержку населения через Центробанк РФ.

Здесь может быть как звонок из «Центробанка», так и реклама в социальных сетях с символикой ЦБ РФ.

В обоих случаях мошенники ссылаются на некий приказ от 20 января 2021 года за подписью некоего заместителя начальника Д.В. Туллина (впрочем, сам приказ и нюансы в его названии не так важны и наверняка могут меняться).

В документе говорится, что каждому россиянину полагается единоразовая денежная выплата (обычно в размере 1 тысячи или 1,5 тысячи рублей) за счет соцвыплаты от Центрального управления Банка Российской Федерации. Все, что нужно для получения заветных денег, – сообщить данные своей банковской карты (включая секретный CVC-код).

Выбирая жертву, мошенники обычно заранее знают, кому звонят (или кому таргетируют рекламные посты в соцсетях). И часто выходят на людей, для которых эти деньги будут как нельзя кстати. Впрочем, согласитесь, кто же откажется от лишних 1,5 тысячи рублей? Тем более если семья большая, сумма получится приличная. Это на руку мошенникам.

Получив все данные карты, аферисты переводят деньги жертвы на свой счет или просто делают покупки на суммы до лимита, не требующего СМС-подтверждения.

ВТОРОЙ СПОСОБ незаконного обогащения со ссылкой на Центробанк более изощренный. Это исключительно телефонное мошенничество, а звонок на телефон жертвы раздается якобы из отделения полиции.

Псевдоследователь информирует вас о том, что вы подозреваетесь в уголовном деле о хищении средств. Причем заявление на вас подал Банк России.

Не дав переварить информацию, вам сообщают, что полиция обязана проверить данные по всем счетам подозреваемого. То есть получить данные всех ваших дебетовых и кредитных карт, а также номера банковских счетов. Естественно, включая CVV-коды, кодовые слова и в некоторых случаях после этого – коды в пришедших на мобильный телефон жертвы СМС-сообщениях. Завладев необходимыми данными, мошенники переводят ваши сбережения на свой счет в считаные минуты.

ТРЕТИЙ СПОСОБ во многом очень похож на предыдущий. Манипуляции осуществляются за счет дозвона, и злоумышленники также представляются сотрудниками правоохранительных органов.

Вот только в мошенничестве они обвиняют не совсем вас. Мол, по данным Центробанка, какие-то мошенники открыли на ваше имя кредит, и по нему имеется долг. Который нужно срочно погасить.

Псевдоследователь подчеркивает, что для прекращения уголовного дела и снятия всех подозрений вам следует срочно погасить задолженность. Но когда найдут преступников, переведенную сумму вернут на счет. При этом суммы могут быть самые разные, но чаще всего они начинаются от нескольких сотен тысяч рублей.

Цель мошенников простая – получить с шокированной жертвы, не желающей иметь проблемы с законом, как можно больше денег. К сожалению, случаи, когда обескураженные люди переводят свои деньги на указанный «следователем» счет, – не редкость.

КАК ЭТОГО ИЗБЕЖАТЬ

В ПЕРВОМ СЛУЧАЕ важно знать несколько вещей.

Во-первых, Правительство РФ, в отличие от многих западных государств, не раздает «вертолетных денег» гражданам.

Да, финансовая поддержка оказывается отдельным категориям граждан в виде единовременных выплат или федеральных надбавок, но такие меры широко рекламируются. Указы и постановления подписываются первыми лицами государства, но никак не заместителями начальников управлений МВД.

Во-вторых, Банк России напрямую не занимается никакими выплатами денег населению. И уж тем более банк никогда не будет отдельно запрашивать данные ваших карт и банковских счетов. Те, кто получал меры поддержки от государства в период пандемии, помнят: все начисления шли через официальные ведомства Правительства, Пенсионный фонд, Министерство социальной защиты. А для получения требовалось подавать заявки посредством портала «Госуслуги». Если же с вас начали требовать персональные данные и данные карт/счетов, знайте: так делают только мошенники.

ВО ВТОРОМ и В ТРЕТЬЕМ СЛУЧАЯХ следует знать, что Центробанк РФ никогда не подает заявления в органы правопорядка в отношении финансовых операций, сделанных без согласия человека.

Даже если против вас действительно возбуждено административное или уголовное дело, сотрудники правоохранительных органов или приставы самостоятельно обратятся в банк для истребования необходимых данных в рамках преследования.

Кроме того, при проведении следственных мероприятий пострадавший или подозреваемый получает повестку о вызове к следователю или дознавателю. А если с вами связываются

по телефону (что в принципе тоже возможно), никто не запрещает вам взять паузу в разговоре, позвонить в дежурную часть и уточнить, действительно ли существует такой сотрудник (который обязан вам представиться в начале разговора).

Как бы то ни было вы не обязаны передавать информацию о своих счетах и банковских картах третьим лицам.

МОШЕННИЧЕСТВО №6: НАВЯЗЫВАНИЕ ЛЮДЯМ УСТАНОВКИ ИЛИ ЗАМЕНЫ ДЫМОУЛОВИТЕЛЕЙ

Дымоуловители, или датчики дыма в квартирах, – дело добровольное. Но знают об этом далеко не все. Да, в новостройках такие системы могут быть установлены изначально, но в старом жилом фонде датчиков дыма в квартирах не предусмотрено. Чем и пользуются мошенники.

В качестве жертв злоумышленники выбирают обычно пенсионеров.

На пороге квартиры возникает человек (или группа лиц), который представляется пожарным, сотрудником МЧС или даже «Водоканала». Порой такой «спасатель» – в униформе с названием организации.

Жителю поясняют, что проводится проверка. И проверка показывает, что в квартире отсутствуют дымоуловители. А это является нарушением закона. Или проверка показывает: датчик есть, но установлен неправильно, у него истек срок эксплуатации и т. д. Основная задача мошенника – завоевать доверие и навязать установку оборудования.

Понятно, что в самих дымоуловителях ничего плохого нет. Более того, в случае задымления помещений они могут спасти жизнь. Но когда за датчики и их установку с вас дерут втридорога или таким агрессивным путем навязывают покупку нового датчика взамен работающего – это натуральное мошенничество.

При этом вам, конечно же, предложат «значительную скидку» и продадут датчик всего за 2–3 тысячи рублей (на самом деле он стоит в 6–8 раз дешевле). А чтобы прикрепить его к потолку, возьмут еще тысячу сверху. Дескать, процесс монтажа сложный, сами не справитесь. В 9 случаев из 10 житель соглашается установить навязанный дымоуловитель. А после монтажа еще и благодарит «спасателей».

КАК ЭТОГО ИЗБЕЖАТЬ

Во-первых, никогда не пускайте в квартиру таких «спасателей».

Ни пожарные, ни МЧС, ни тем более «Водоканал» не продают никаких датчиков таким образом. Никто из них не ходит по квартирам и не навязывает установку подобного оборудования, тем более по доброте душевной и с «огромными скидками». Поэтому, увидев таких умельцев, что называется, гоните их в шею!

Во-вторых, установка дымоуловителей – дело сугубо добровольное.

За их отсутствие никакой ответственности вы не понесете. По крайней мере пока не будет утверждена соответствующая законодательная база. Если же такие датчики в вашей квартире установлены застройщиком (то есть присоединены к системам дома), конечно, не следует их демонтировать или закрывать к ним доступ.

В-третьих, вопрос цены. Даже если вы озаботились установкой датчика дыма, не следует соглашаться на расценки таких

доброхотов. В среднем стандартный дымовой датчик стоит от 300 до 500 рублей. Более усовершенствованные модели (например, со встроенным GPS-модулем) обойдутся вам уже дороже – в среднем от 1,5 до 3 тысяч рублей. Установка такого оборудования на потолок возможна самостоятельно и не занимает много времени.

МОШЕННИЧЕСТВО №7: НАВЯЗЫВАНИЕ ЛЮДЯМ УСТАНОВКИ ГАЗОАНАЛИЗАТОРОВ

Схема мошенничества похожа на предыдущую. Только вместо продавцов дымоуловителей здесь фигурируют продавцы газоанализаторов (или датчиков утечки газа). Жертвами становятся жители газифицированных домов.

Как и в случае с дымоуловителями, пока не существует закона, обязывающего жителей газифицированных домов устанавливать в квартирах газоанализаторы.

От людей лишь требуется следующее: содержать газовое оборудование в надлежащем состоянии и чистоте, сохранять в целостности установленные на газовое оборудование пломбы и в целом быть осведомленными о всех возможностях использования газового оборудования.

Однако мошенники эти требования решили дополнить. И пытаются убедить жертву, что обладатель газовой плиты просто обязан иметь в квартире работающий датчик утечки газа.

Убеждают население псевдосотрудники МЧС или газовой службы. Цена на новенький (и не факт, что рабочий) датчик

утечки газа варьируется от 5 до 10 тысяч рублей. Притом, что его реальная стоимость не превышает 2 тысяч. Если житель квартиры начинает вздыхать, что цена слишком высока, ему рассказывают сказку, что в случае утечки газа чудо-аппарат тут же сообщит о проблеме в газовую службу. О том, что без подключения анализатора к домовым системам добиться этого технически невозможно, покупателю не докладывают.

И вот датчик установлен. Рад хозяин квартиры. Рады мошенники, ведь они только что заработали кругленькую сумму. Из хорошего в этом случае на самом деле возможно только одно: если газоанализатор окажется работающим. Зачастую мошенники устанавливают пустой пластиковый корпус с мигающей лампочкой. Пользы от такого устройства нет никакой.

КАК ЭТОГО ИЗБЕЖАТЬ

Лучший из возможных вариантов – не открывать двери незнакомцам. Что касается газоанализаторов, помните: никакие датчики утечки газа не оповестят специализированную службу о наличии проблемы.

Да, представители газовой службы проводят в домах проверку оборудования. Но, как правило, о таких мероприятиях собственникам сообщает либо сама служба, либо управляющая организация. Дата и время обхода согласовываются и актируются. И никто в ходе проверки не станет требовать или навязывать вам покупку подобных приборов.

Если с установленным газовым оборудованием имеются проблемы, его ремонт или переустановка производятся исключительно газовиками, поскольку неправильные действия могут повлечь опасность не только для вас, но и для всего дома.

Также еще раз напомним: наличие газоанализатора в квартире пока не является узаконенной нормой. Если это случится, до каждого из владельцев газифицированной квартиры информа-

ция будет доведена управляющими организациями или представителями местных властей.

Вдобавок к этому всегда смотрите на цену товара, который вам предлагают купить.

Дорого? Возникли сомнения? Тогда, как говорится, загуглите. Посмотрите, сколько стоит такое оборудование в интернете. И вы убедитесь, что овчинка выделки не стоит.

МОШЕННИЧЕСТВО №8: БЕСПЛАТНАЯ РАЗДАЧА СИМ-КАРТ И ИХ ДАЛЬНЕЙШИЙ ПЕРЕВЫПУСК

На улице к вам подходит человек и предлагает купить сим-карту. А то и не одну. Причем любого сотового оператора. Это не значит, что такая покупка обязательно в будущем выйдет вам боком. Сим-картами бойко торгуют у вокзалов, в переходах метро, поблизости от мест скопления людей. Чаще всего покупателями таких симок становятся туристы или иногородние приезжие.

Но случается и так, что продают вам сим-карту вовсе не для того, чтобы вы оставались на связи в другом регионе страны. Это еще один способ мошенничества. Сим-карту вам продали, чтобы в будущем перевыпустить ее под видом потери или кражи. Обратиться в будущем в салон оператора связи для получения новой симки взамен старой для хозяина сим-карты не составит особого труда.

Зачем это ему, спросите вы. Все просто. Перевыпустив сим-карту, человек получает доступ к вашему номеру. По крайней мере на какое-то время. А это значит, что мошенник не про-

сто сможет получать на свой телефон звонки и СМС от ваших контактов (которые будут думать, что пишут вам), но и, зная другие ваши личные данные, попытается получить доступ к вашим социальным сетям и приложениям, авторизовываясь по номеру телефона. Самое опасное, если к телефону привязаны банковские карты и онлайн-приложения, – в этом случае ему будет открыт доступ к вашим счетам.

А дальше стандартные сценарии. Например, в соцсетях авторизовавшийся под вашим номером телефона мошенник сможет разослать вашим друзьям сообщения с просьбой занять немного денег и перевести их на телефон (или даже на нужный банковский счет). При этом многие доверчивые люди могут с ходу поверить ему и действительно самостоятельно лишить таким образом себя части финансов. Или же это может быть рассылка слезной истории о том, что «мои родители или ребенок попали в страшную аварию и срочно нужны деньги». Ведь совести обычно у таких людей мало или нет вовсе. А про возможность получения доступа к интернет-банку и последующую возможность управлять вашими деньгами, думаем, вы уже сами догадались.

Все это, конечно, мошенничество. Кража личной информации и тем более финансов – преступление. Однако само по себе обладание вашей сим-картой преступлением с точки зрения законодательства считаться не будет. Поскольку приобретали вы изначально сим-карту с данным номером не официально, а с рук. А значит, не заключали с сотовым оператором никакого договора и не предоставляли ему свой паспорт.

Да и вообще, как правило, найти после совершения такого преступления человека очень сложно. Во-первых, подобных случаев по стране наблюдается достаточно много. А, во-вторых, обычно такие люди очень осторожны и стараются как можно скорее получить свою выгоду и избавиться от злополучной сим-карты.

КАК ЭТОГО ИЗБЕЖАТЬ

Тут все просто. Не нужно покупать неофициальные сим-карты или сим-карты с рук. Приобретайте их только в официальных салонах связи и магазинах. Тогда маловероятно, что кто-то сможет воспользоваться вашей сим-картой, за исключением случаев, когда ваш телефон или сим-карта украдены или потеряны.

Однако все равно будьте бдительны! Иногда встречаются попытки мошенников перевыпустить сим-карту по поддельным документам. Что, в случае успеха, чревато теми же проблемами, что описаны выше. Поэтому, если вы подозреваете подобное, лучше сходите в салон вашего мобильного оператора и проверьте это наверняка.

МОШЕННИЧЕСТВО №9: НОВЫЕ МЕТОДЫ МАСКИРОВКИ ФИШИНГОВЫХ САЙТОВ

В первой брошюре, посвященной видам мошенничества, мы уже затрагивали тему фишинговых сайтов. То есть сайтов, которые порой как две капли воды похожи на оригинальные сайты банков, сфер услуг и пр., но по факту являются подделкой. Напомним, что сегодня фишинговые махинации являются самым распространенным киберпреступлением. Цель которого одна – заставить вас перейти на ложный сайт банка / сервис оплаты.

Но, как известно, прогресс не стоит на месте. И сегодня мошенники создали новый способ маскировки фишинговых сайтов в России. Который не только облегчает злоумышленникам работу, но и значительно повышает шансы преступников на успех, защищая их при этом от систем информационной безопасности.

Суть этого метода заключается в таргетировании письмами, ссылками и постами, ведущими на такие сайты, каждого пользователя, основываясь на различных данных и «следах» в интернете, которые оставляет жертва. Жертвами в основном становятся индивидуальные предприниматели. А основной платформой выступают слабозащищенные смартфоны.

Мошенники отбирают жертву по модели телефона, данным геолокации, браузеру, которым человек пользуется. При этом, если человека провести не удается, при переходе на такой сайт он увидит просто так называемый сайт-заглушку или вообще ошибку при открытии интернет-страницы.

Если же переход осуществлен «успешно», мошенники по принципу считывания вводимых данных стараются заполучить как можно больше личной информации от пользователя. Например, если это ложный сайт банка, киберпреступники могут завладеть вашими логином и паролем от личного кабинета. Та же история – и с социальными сетями, сайтами государственных услуг или прочими платформами, от которых зависят ваши финансы, личная информация и другие персональные данные.

КАК ЭТОГО ИЗБЕЖАТЬ

Алгоритм противодействия кибермошенникам достаточно простой. Прежде всего – никогда не переходите по сомнительным интернет-ссылкам. Неважно, будете вы это делать с компьютера или смартфона – риск одинаково велик. При этом помните, что ссылка может «упасть» не только в виде спама в почтовый ящик.

При совершении каких-либо действий на сайте банка или в приложении внимательно осмотрите домен сайта (чтобы он полностью совпадал с доменом официального банковского сайта до каждой буквы, цифры или знака). Не будет лишним пройтись по разным вкладкам, посмотреть на шрифты, анимации. Мошенники обычно подделывают лицевую страницу и не углубляются в копирование подвкладок и ассортимента сервисов.

Также не экономьте на установке антивирусных программ как на компьютерах, так и на смартфонах. Многие мошеннические программы могут скрытно устанавливаться и подстраиваться под определенные сайты/приложения через вирусные ссылки. Лучше один раз заплатить за лицензионный антивирус, чем потом понести большие финансовые потери.

И не забывайте обновлять ваши мобильные и операционные системы до последних версий. Помните, что цель обновлений ПО – не только устранение «глюков» или новые смайлики. Иногда обновления закрывают важные бреши в системе безопасности ваших смартфонов и ПК. Поэтому не забывайте регулярно обновлять операционную систему. Что касается приложений, скачивайте их в официальных онлайн-магазинах, где они проходят проверку на вирусы.

МОШЕННИЧЕСТВО №10: ОПАСНЫЙ СПАМ НА ЭЛЕКТРОННОЙ ПОЧТЕ И ВЫМОГАТЕЛЬСТВО ДЕНЕГ

Пожалуй, это самый свежий вид электронного интернет-мошенничества. Хотя сама по себе схема известная и отчасти включает в себя методы фишинга, угрозы и обещания выгоды жертве. Однако ее исполнение целиком и полностью зависит от конкретного примера. Ниже мы приведем самые распространенные примеры такого мошенничества.

Отметим, что объединяет их одно – преступники в данном случае всегда действуют через электронную почту. И в 2020–2021 годах используют они такой метод особенно часто, таргетируя едва ли не каждый первый электронный почтовый ящик.

ПЕРВЫЙ СПОСОБ такого вида обмана связан с якобы выплатой компенсаций.

Вам на почту могут прийти электронные письма, в которых будет предлагаться перейти по специальной ссылке на сайт либо Единого компенсационного центра, либо Центра материальной поддержки. Также возможны переходы и на сайты других «аттракционов неслыханной щедрости» – суть от этого не меняется.

Прикрываться мошенники здесь могут либо неким исполнительным приказом по начислению человеку социальных компенсаций, либо просто фондом, который производит выдачу денежных возвратов (и даже якобы не одну). Важно понимать, что любые подобные сообщения – дело рук мошенников, которые хотят, чтобы вы прошли по их ссылкам на заранее подготовленные сайты, где с вами даже якобы сможет пообщаться юрист.

Естественно, после недолгой консультации с роботом, прикидывающимся реальным человеком (или даже без такой консультации), вас попросят ввести определенные данные, после чего запустится заранее сгенерированное представление с якобы вычислением размера именно вашей денежной выплаты. Которая может составить от десятка до нескольких сотен тысяч рублей.

В заключение с человека потребуют лишь оплатить услуги юриста, после чего компенсацию обещают выслать на указанный вами счет. Но вот незадача: как только вы переведете деньги за псевдоуслуги псевдоюристов, ничего не произойдет. Никакую компенсацию вы не получите. Зато подарите мошенникам минимум несколько сотен рублей.

Казалось бы, потери невелики. Но не забывайте, что подобным образом мошенники таргетируют своим опасным спамом сотни тысяч электронных ящиков ежедневно. И ведутся на такие схемы достаточно большое количество неподкованных пользователей. При этом даже на один ящик могут приходить по несколько подобных писем, но от разных организаций. Поэтому навар от такого массового обмана оценивается десятками миллионов рублей.

Ниже для наглядности мы приведем несколько реальных примеров таких электронных спам-писем.

ПРИМЕР СПАМ-ПИСЬМА ПО ПСЕВДОКОМПЕНСАЦИЯМ №1

Госуслуги. Вам полагается компенсация за истекший период!

«Здравствуйте! Вынесено постановление о начислении социальных компенсаций 26846/10/724033-ИП от 2020-11-20, исполнительный приказ №2-115/2021-968 от 2021-01-20.

Для оформления обращайтесь в личном кабинете к ведущему юристу: ГОНЧАРОВА Л.В. //Центральное РОСП (код отдела: 55453).

*Идентификация по данным документа «СНИЛС» №********, указанного в личном кабинете.*

Активируйте письмо и перейдите на портал (для активации письма нажмите кнопку «Включить» вверху письма или кнопку «Не спам!»)».

ПРИМЕР СПАМ-ПИСЬМА ПО ПСЕВДОКОМПЕНСАЦИЯМ №2

Коалиция по выплатам. Вы владелец крупной суммы деньжат!

«Хотим Вас известить, что наш фонд открывает вторую волну выдачи денежных возвратов!

Вам требуется разрешить обращение и подождать пару секунд. Расчет Вашей суммы возврата будет получен.

Щелкните сюда и зайдите на официальный сайт».

ПРИМЕР СПАМ-ПИСЬМА ПО ПСЕВДОКОМПЕНСАЦИЯМ №3

Альянс выплат гражданам. Срок оформления заявок на зачисление выплаты ограничен!

«Согласно постановлению №1846УМП-3117КФВ, Вам полагается единоразовая выплата денежных средств.

ВНИМАНИЕ! Исполнить заявку необходимо в течение пары дней, иначе нам придется деактивировать Ваш профиль!

Для этого перейдите на сайт и оставьте обращение».

ВТОРОЙ СПОСОБ спам-обмана очень похож на первый, но ключевой механикой в нем выступают не социальные выплаты или компенсации, а старая, добрая лотерея «Гослото».

Неважно, покупали ли вы лотерейные билеты или нет, на вашу электронную почту могут упасть странные сообщения.

Рассылка осуществляется якобы от ОАО «Гослото» или некоего SuperLotto. Письма еще в своих темах кричат о том, что вам полагается бесплатный лотерейный билет. И все, что вам нужно, – перейти по ссылке в письме и поучаствовать в розыгрыше. Конечно же, вы можете выиграть даже 1 млрд рублей!

Переходя по ссылке, человек сначала становится участником псевдорозыгрыша. А потом открывается окно с роботом, маскирующимся под сотрудника «Гослото». Где девушка с красивой картинки спешит поздравить вас с выигрышем, составлять который может от сотен тысяч до миллионов рублей.

Казалось бы, вот оно, везение! И все, что нужно, чтобы получить заветный куш, – это ввести полные данные вашей банковской карты. Которые, как известно, мошенникам нужны отнюдь не для того, чтобы порадовать вас деньгами. А, наоборот, отнять у вас то, что лежит на счете и было нажито непосильным трудом.

По аналогии с первым способом обмана подобные сообщения также могут отличаться в названиях отправителей или даже в своем содержании. Также на вашу электронную почту может прийти не одно такое сообщение.

Ниже для наглядности мы приведем несколько реальных примеров таких электронных спам-писем.

ПРИМЕР СПАМ-ПИСЬМА ПО ПСЕВДОВЫИГРЫШУ ОТ «ГОСЛОТО» №1

ОАО «Гослото». Вам полагается бесплатный лотерейный билет.

«Здравствуйте!

В честь своего 25-летия «Гослото» решило подарить Вам бесплатный лотерейный билет с возможностью выиграть до 1 000 000 000 рублей! Билет является электронным и привязан к электронной почте получателя. Чтобы активировать свой билет, перейдите на страницу розыгрыша.

Страница розыгрыша.

Желаем удачи! Ваше «Гослото»

ПРИМЕР СПАМ-ПИСЬМА ПО ПСЕВДОВЫИГРЫШУ ОТ «ГОСЛОТО» №2

ОАО «Гослото». Ваш билет №9042-6559-3447-8327

«Здравствуйте!

В честь своего юбилея «Гослото» дарит Вам бесплатный лотерейный билет!

Денежные выигрыши первых нескольких туров – самые крупные и могут составлять от нескольких десятков и сотен тысяч до нескольких миллионов рублей.

Проверьте билет, чтобы не упустить свой выигрыш! Получить бесплатный билет здесь – https://inlnk.ru/rZex4

Возможно, вам нужно будет включить ссылку, чтобы она была активна».

ПРИМЕР СПАМ-ПИСЬМА ПО ПСЕВДОВЫИГРЫШУ ОТ «ГОСЛОТО» №3

SuperLotto. У Вас (1) новое сообщение №82852991

«Добрый день!

Вам доступен подарочный билет к юбилейному тиражу по данной ссылке:

Подробнее здесь

Желаем удачи!».

ТРЕТИЙ СПОСОБ опасного спама значительно отличается от первых двух по своей тематике и содержанию. Здесь мошенники не умасливают жертву и не используют никаких гиперссылок, ведущих на опасные сайты для вымогания денег. Еще в теме письма преступники сразу переходят к угрозам, запугиванию и обычно вымогают деньги в криптовалюте (в биткойнах) посредством их перевода на анонимный криптокошелек. Обычно вымогают от 500 до 700 долларов США.

В качестве причины, по которой жертва должна перевести мошеннику деньги (обычно сделать это необходимо в течение двух суток), является псевдовзлом вашего компьютера. Якобы человек взломал ваш роутер, проник в компьютер и не просто завладел всеми вашими данными, но и получил доступ к веб-камере, а также возможность видеть картинку с монитора.

Если вкратце, злоумышленник намекает в письме на то, что с помощью таких возможностей он сумел «нарыть» на вас компромат. Который, естественно, разошлет всем знакомым и друзьям, чьи контакты он тоже якобы заимел через ваш компьютер. А чтобы этого не произошло, придется заплатить. Как говорится, ничего личного – просто бизнес…

Естественно, кто-то над таким сообщением лишь посмеется. Поскольку сама схема взлома, которую описывает мошенник, требует не только определенных навыков и времени, но и по многим причинам просто невозможна. По крайней мере в ковровом многотысячном масштабе. Однако некоторые люди на такую угрозу реагируют. И готовы заплатить любые деньги, чтобы вернуть себе приватность.

Ниже для наглядности мы приведем реальный пример такого электронного спам-письма.

ПРИМЕР СПАМ-ПИСЬМА ПО ПСЕВДОВЗЛОМУ ВАШЕГО КОМПЬЮТЕРА

Скверные новости для вас. Pixel – 05601356, или Крайнее предупреждение!

«Добрый день! У меня для вас плохие новости. 05.10.2020 – в этот день я взломал вашу операционную систему и получил полный доступ к вашей учетной записи. Конечно, вы можете сменить пароль. Но мой софт перехватывает каждый раз, когда вы его меняете.

Как я это сделал: в программном обеспечении роутера, через который Вы выходили в интернет, было слабое место. Я просто взломал этот роутер и поместил на него свой вредоносный код. Когда Вы выходили в интернет, мой троян был установлен на ОС вашего устройства. После этого я сделал полную копию вашего диска (у меня есть вся ваша адресная книга, история просмотра сайтов, все файлы, номера телефонов и адреса всех ваших контактов).

Месяц назад я хотел заблокировать ваше устройство и попросить небольшую сумму в биткойнах для разблокировки. Но я посмотрел сайты, которые вы регулярно посещаете, и был шокирован увиденным!!! Я имею в виду сайты для взрослых. Я хочу сказать – Вы большой извращенец. Ваши фантазии не имеют ничего общего с нормальным восприятием обычного человека. И у меня появилась идея…

Я сделал скриншот сайтов для взрослых, на которых Вы развлекаетесь (вы понимаете, о чем это, да?). После этого я сделал скриншоты, как Вы весьма необычно себя удовлетворяете (используя камеру вашего устройства), и склеил их. Получилось потрясающе! Это впечатлит любого, тем более ваших знакомых!

Я знаю, что вы не хотели бы показывать эти скриншоты своим друзьям, родственникам или коллегам. Я думаю, что $700 (USD) – чрезвычайно маленькая сумма за мое молчание. Кроме того, я и так долго шпионил за вами, потратив много времени! Платите

ТОЛЬКО в биткойнах! Мой кошелек BTC: 14s4i1WRPQ4BdwGtt38oumwdebKdvVdUfG. Вы не знаете, как использовать биткойны? Введите запрос в любой поисковой системе (Google или Яндекс): «Как пополнить BTC кошелек». Это очень легко.

На это я даю вам два дня (48 часов) с момента открытия этого письма. Pixel – 05601356. Учтите, как только вы откроете это письмо, сработает таймер. И время пойдет. После оплаты мой вирус и все скриншоты с вашими развлечениями будут автоматически уничтожены. Если я не получу от вас указанную сумму, то ваше устройство будет заблокировано, и все ваши контакты получат скриншоты с вашими пошлыми удовольствиями.

Я надеюсь, вы понимаете свою ситуацию. Не пытайтесь найти и уничтожить мой вирус! Все ваши данные, файлы и скриншоты уже загружены на удаленный сервер. Не пытайтесь связаться со мной (это невозможно, так как адрес отправителя генерируется случайным образом). Различные службы безопасности вам не помогут; форматирование диска или уничтожение устройства не поможет, так как ваши данные уже находятся на удаленном сервере.

P.S. Вы моя не единственная жертва. И я гарантирую вам, что я не буду беспокоить вас снова после оплаты! Это слово хакера. Я также прошу вас регулярно обновлять ваши антивирусы в будущем. Таким образом, вы больше не попадете в подобную ситуацию. Не держите на меня зла! У каждого своя работа».

КАК ЭТОГО ИЗБЕЖАТЬ

Совет по всем трем перечисленным способам мошенничества является универсальным.

Во-первых, не стоит открывать подозрительные спам-письма! А если вы это сделали, не переходите по встроенным в них гиперссылкам.

Лучше всего такие сообщения из почтового ящика сразу удалять. Помните: бесплатный сыр бывает только в мышеловке! Особенно если речь идет о многотысячных и даже миллионных выигрышах или компенсациях.

Кроме того, если вы действительно имеете право на получение компенсации или социальных выплат от государства, вам предстоит заполнять определенные бумаги, преодолеть определенный бюрократический процесс. В два клика на непонятном сайте с российским флагом на фоне это не делается!

Во-вторых, для участия в лотерее вы как минимум должны приобрести реальный лотерейный билет за реальные деньги! Иначе «Гослото» и другие подобные компании ничего бы не зарабатывали. И вероятность получить выигрыш даже в несколько тысяч рублей (не говоря уже о миллионах) весьма невелика. С ходу по одному клику вы также никогда не получите лотерейных денег!

В-третьих, касательно угроз взлома компьютера, само по себе это возможно. Но вероятность, что на взлом компьютера обычного человека (причем взлом якобы производится через роутер, от которого требуется находиться в непосредственной близости) мошенник будет тратить уйму времени, крайне мала.

А с учетом того, что такие сообщения приходят тысячами на почтовые ящики разных людей в разных населенных пунктах, взламывать всех и каждого в таком количестве просто невозможно.

Не открывайте подозрительные письма и не переходите на подозрительные сайты. Даже чисто из любопытства. Не экономьте на установке антивирусных программ как на компьютерах, так и на смартфонах. Многие мошеннические программы могут скрытно устанавливаться и подстраиваться под определенные сайты/приложения через вирусные ссылки или сайты. Лучше заплатить за лицензионный антивирус, чем потом расплачиваться большими финансовыми потерями и сожалениями.

ПОДВОДИМ ИТОГИ

Разумеется, это далеко не все виды мошенничества, которые, к сожалению, активно используют злоумышленники в современном мире. Однако на описанные десять видов приходится большая доля современных видов мошенничества.

Очередные новые схемы и уловки мы обязательно разберем в наших инструкциях из цикла «Как обезопасить себя и своих близких от мошенников». Напомним: это уже второй большой сборник Центров защиты прав граждан на тему мошенничества. Первый вы можете прочитать на сайте **справедливо-центр.рф** в разделе **ФИНАНСЫ**.

Мы надеемся, что представленные алгоритмы уберегут вас от потери сбережений и нервных потрясений.

Главное – запомните **ТРИ ПРАВИЛА**, которые помогут либо избежать контакта с мошенниками, либо извлечь из этого правильные выводы:

ВО-ПЕРВЫХ, от столкновения с мошенниками никто не застрахован, это **МОЖЕТ ПРОИЗОЙТИ С КАЖДЫМ**. Не стоит относиться к этому с позиции «со мной этого точно никогда не случится». Повторим словами известной поговорки – не зарекайся!

ВО-ВТОРЫХ, практически любой вид мошенничества **МОЖНО И НУЖНО ИЗБЕГАТЬ.** Необходимо быть бдительным, стараться дистанцироваться от навязчивых сомнительных предложений, научиться распознавать попытки вас «обработать».

В-ТРЕТЬИХ, если вы все-таки стали жертвой мошенников, **НЕ ОТЧАИВАЙТЕСЬ И ПОСТАРАЙТЕСЬ СДЕЛАТЬ ИЗ ЭТОГО ВЫВОДЫ.** Используйте пережитое в качестве урока и не повторяйте своих ошибок в будущем. Обязательно расскажите о своем опыте друзьям и близким, чтобы они также не попались на удочку любителей разбогатеть за чужой счет.

ЦЕНТР
ЗАЩИТЫ ПРАВ ГРАЖДАН
справедливо-центр.рф
8-800-755-55-77

СПРАВЕДЛИВОЕ РАДИО

Справедливое радио
на сайте домовой-совет.рф

YouTube-канал
«Центр справедливости»

ДОМОВОЙ СОВЕТ

Газета «Домовой совет»
домовой-совет.рф

Телефон горячей линии
8 800 755 55 77

Сайт Фонда
«Центр защиты прав граждан»
справедливо-центр.рф

Пособие: КАК ОБЕЗОПАСИТЬ СЕБЯ И БЛИЗКИХ ОТ МОШЕННИКОВ. ЧАСТЬ 2
Изготовитель: ООО «Производственный комбинат «Имидж», ИНН 5030092946
143306, Московская область, г. Наро-Фоминск, ул. Ленина, д. 28 офис 3
Заказчик: Фонд «Центр защиты прав граждан», ИНН 9710010183.
Тираж: 0000 экз. 2021 год
Распространяется бесплатно

В ТРУДНОЕ ВРЕМЯ РЯДОМ С ТОБОЙ!