«Кредиты и займы – не зло, а социальная мобильность». Эксперт о защите от уловок черных кредиторов

Черные кредиторы... Пожалуй, это и есть то самое зло для современного заемщика, в борьбе с которым ему надо надеяться, прежде всего, только на себя самого. И дело не в том, что правоохранительные органы никогда не смогут полностью искоренить эти мошеннические схемы, а в том, что когда дело дойдет до их вмешательства, есть реальный шанс потерять все. Безвозвратно. Тема нелегальных кредиторов активно обсуждается в социальных сетях, про них снято много видеороликов и даже фильмов-расследований. Их схемы изучены. Четкое соблюдение нескольких простых правил, позволит не стать жертвой «черных кредиторов». О них «ФедералПресс» рассказал президент Национальной ассоциации профессиональных коллекторских агентств (НАПКА), эксперт проекта финансовой грамотности Минфина РФ Эльман Мехтиев.

«Чтобы избежать обмана, нужно помнить пять простых правил.

Первое – не занимаем деньги у незнакомых (или недавно ставшими знакомыми) физических лиц под расписку. Действия по возврату такой просроченной задолженности на досудебной стадии никак не регулируются и потому находятся вне государственного контроля, а заемщики – вне защиты со стороны надзорных органов.

Вы уверены, что ваш кредитор пойдет сразу же и только в суд?

Второе – проверяем наличие компании-кредитора в реестре / «списках» ЦБ (cbr.ru). Все банки имеют лицензию Банка России. Все МФО состоят в реестре Банка России. Но проверять надо не только совпадение названия, но и номер лицензии / дату записи в реестре.

Где гарантия, что если название кредитора «немного отличается» от указанного в реестре, его действия не будут отличаться от разрешенных законами?

Третье – внимательно изучаем сайт компании. Несколько лет назад Банк России договорился с одним из ведущих Интернет-поисковиков о маркировке компаний из реестра ЦБ прямо в адресной строке. Таким образом, удалось в разы упростить процесс проверки организации для физических лиц. Не будет лишним посмотреть на сайте компании информацию о лицензии. Как правило, компании из реестра ЦБ не только указывают номер лицензии, но и публикуют сканы документов.

Будьте внимательны – нередки случаи, когда недобросовестные кредиторы маскируются под легальные компании. Они могут использовать крайне схожую символику, создавать сайты-близнецы. С виду, на первый взгляд, кажется все то же самое, однако на их сайтах нет никакой информации, подтверждающей право ведения деятельности или же она просто не соответствует тому, что есть о данной компании (если есть) на сайте ЦБ.

Вы уверены, что выражение «доверяй, но проверяй» не имеет отношения к вашим финансам?

Четвертое – читаем договор. К сожалению, по статистике 70% заемщиков в лучшем случае бегло просматривают страницы, проверяя по просьбе сотрудника лишь свои паспортные данные и реквизиты счета или платежной карты. Такая легкомысленность впоследствии может дорого обойтись, если кредитор сознательно использует невнимательность и торопливость. Поэтому перед подписанием стоит внимательно изучить каждый пункт договора.

Особое внимание стоит уделить условиям предоставления ссуды и не забыть посмотреть в правый верхний угол первой страницы, где должна быть указана полная стоимость кредита (ПСК). Это должен быть именно договор о предоставлении кредита или займа, но ни в коем случае не договор купли-продажи.

Помните, что, если вы искали кредит или заём, значит надо брать кредит или заём, а не подписывать сложные сделки, в которой вы то ли продавец, то ли покупатель, то ли инвестор, то ли займодавец. Иначе придя за деньгами, можно уйти по собственной воле с деньгами в кармане, но уже без имущества (квартиры или машины).

И даже если «кредиторы» никуда не исчезнут, суды будут на их стороне – вы же подписали такие договоры «в своем уме и твердой памяти».

Пятое – ищем отзывы. В современном мире, в эпоху развития Интернета, будет не лишним ознакомиться с отзывами о компании, куда Вы собираетесь обращаться за займом. Информация с 2-3 сайтов позволит сформировать мнение о компании и о методах ее работы.

Будьте внимательны – много положительных однотипных отзывов может означать и то, что компания сама потратила много сил и даже денег на написание таких отзывов.

Подводя итоги, хочется сказать: кредиты и займы – не зло, а социальная мобильность, инструмент, который позволяет добиваться целей раньше, но только в том случае, если цели стоят того, а деньги берутся у тех, кто работает по букве закона».

Почему нельзя сохранять данные банковской карты в интернет-магазинах?

Многие интернет-магазины предлагают сохранить данные банковской карточки — чтобы не вводить их каждый раз, когда совершаешь покупки. Эксперты по финансовой грамотности говорят, что этого лучше не делать. Все дело в регулярных утечках персональных данных из банков, отелей, даже медицинских клиник и ресторанов.

«Банковская карта представляет собой „кусок пластика“, имеющий определенные реквизиты: это номер карты, в котором заложена информация о наименовании платежной системы, типе карты и др., имя и фамилия владельца, дата окончания действия карты — месяц и год, защитный чип, который представляет из себя сложное устройство со своим процессором, памятью и множеством других элементов, которые взаимодействуют между собой. На оборотной стороне карты есть CVC/CVV2-код, состоящий из трех (иногда из четырех цифр). Если эти данные по отдельности попадут к постороннему лицу, это не несет для вас никакой опасности. Однако если эта информация в совокупности, а особенно CVC/CVV2 код, попадет к третьему лицу, вы можете лишиться своих средств на карте», — предупреждает консультант по финансовой грамотности проекта «вашифинансы.рф» Игорь Григорьянц.

Нет никакой гарантии, что организации, из которых сейчас утекают паспортные данные или номера телефонов клиентов, со временем не допустят утечку данных чужих банковских карт.

Еще один риск для утечки данных карточки — фишинговые сайты, которые создают мошенники и которые копируют сайты известных магазинов, банков, сервисов и проч. «После попадания на отдельную страницу пользователь указывает свои персональные данные, к которым и получает доступ мошенник, а далее — полный доступ к банковским картам, счетам и электронным кошелькам. Когда были объявлены меры поддержки семей и выплаты на детей до 16 лет, количество „сайтов-близнецов“ госуслуг и Пенсионного фонда выросло в разы», — напоминает эксперт Национального центра финансовой грамотности Светлана Ефимкина.

Как спастись от мошенников?

Распознать поддельный сайт не очень сложно. «Для начала проверьте доменное имя сайта, где вы собираетесь совершить покупку. Там могут содержаться ошибки, отличающие его от доменного имени настоящего сайта. Проверьте наличие SSL-сертификата — шифрование для передачи данных пользователя. Адреса сайтов с таким сертификатом должны начинаться на „https://“. А вот если адрес сайта начинается на „http://“, то стоит задуматься е его подлинности. Проверьте сайт на наличие грамматических, орфографических и дизайнерских ошибок. Если данный сайт вызвал у вас какие-либо подозрения — ни в коем случае не пользуйтесь их услугами», — предупреждает Григорьянц.

Обязательно загляните на страничку с контактами. Хоть магазин и онлайновый, он у него все равно должен быть физический адрес. Введите этот адрес на Google-картах — сервис покажет, действительно ли здесь находится нужный интернет-магазин.

Есть еще один способ: пробить интернет-магазин как юридическое лицо. Сделать это можно на одном из следующих сайтов: https://egrul.nalog.ru/, https://www.rusprofile.ru/ и https://fek.ru/. Здесь вы увидите, какой вид деятельности заявлен интернет-магазином. Если, например, вы собираетесь купить кроссовки в спортивном магазине, а вид деятельности у него «сантехнические услуги», это повод поискать другого продавца.

Наконец, проверьте наличие пользовательских соглашений, условия оплаты и доставки — вся эта информация обязательно должна быть на сайте интернет-магазина. А вот чего не должно быть, так это отсылок в пользовательском соглашении на сторонние компании, которые не имеют отношения к данному сайту.

Игорь Григорьянц рекомендует завести отдельную банковскую карту, привязанную к отдельному счету для оплаты покупок в интернете. По словам Ефимкиной, это может быть виртуальная карта, которую сейчас предлагают в большинстве банков.

«Переводите на эту карту для оплаты интернет-покупок каждый раз ровно столько, сколько вам нужно для оплаты в этот раз, и не храните на ней излишки средств», — подсказывает Григорьянц.

«Основной счет, на котором лежат денежные средства, должен быть отдельно и не должен быть привязан ни к каким банковским картам», — добавляет Ефимкина.

Алло, это аферисты? Что отвечать мошенникам, чтобы они больше не звонили

Более четверти владельцев банковских карт в зоне риска стать жертвой аферистов — они могут назвать мошенникам персональные данные своих карточек (срок действия и CVC-код), говорится в материалах аналитического центра Национального агентства финансовых исследований (НАФИ).

Оказывается, лишь 10% наших соотечественников знают, какие данные карты можно сообщать сотруднику банку: ее номер, фамилию и имя держателя.

С мошенниками сталкивались 31% россиян, чаще всего злоумышленники звонили им по телефону и пытались вытянуть персональную информацию с помощью социальной инженерии. Как аферисты крадут деньги и что отвечать, когда звонят из «службы безопасности» банка, рассказывает АиФ.ru.

Миллионные манипуляции

Самая популярная (и самая действенная) мошенническая схема выглядит следующим образом: гражданину звонят из банка и сообщают, что с его счета была совершена сомнительная операция, например, перевод кругленькой суммы в другой регион или даже в другую страну.

Злоумышленники активно применяют методы социальной инженерии: на них приходится почти две трети всех хищений с банковских счетов россиян, свидетельствуют данные Центрального банка РФ. Аферисты заранее собираются необходимую информацию о потенциальной жертве, с постоянными утечками персональных данных граждан это не так сложно. Часть мошенники звонят своим жертвам рано утром или, наоборот, в разгар рабочего дня, чтобы застать человека врасплох, не дать ему возможности как следует обдумать происходящее.

«Уверенный и спокойный мужской голос обращается к вам по имени и отчеству, чтобы вызвать доверие, представляется сотрудником службы безопасности банка и действует по одному из основных сценариев:

- сообщает о подозрительной активности с вашей банковской картой. Например, о попытке перевести крупную сумму или о запросе на банковскую операцию из другого региона, где вы никогда не были. В целях отмены несанкционированной операции просит назвать полный номер вашей банковской карты и код подтверждения из смс, поступившем от банка. Аферист сам предупреждает вас, что смс-код никому нельзя сообщать и просит ввести его в тоновом режиме, чем усыпляет вашу бдительность;
- сообщает о попытке несанкционированного списания денежных средств с вашего счета и предлагает перевести деньги на «безопасный счет», который, естественно, принадлежит мошенникам. Если вы не соглашаетесь, может пригрозить штрафом за отказ перевода денежных средств;
- сообщает о выявлении вредоносного программного обеспечения на вашем смартфоне. Для устранения просит предоставить доступ к устройству,

установив на гаджет программу удаленного доступа TeamViewer или Anydesk. Вы устанавливаете программу и обеспечиваете непосредственный доступ злоумышленников к вашему банковскому счету», — перечисляет эксперт Национального центра финансовой грамотности, консультант по финансовой грамотности проекта вашифинансы.рф Наталья Шумакова.

Граждане верят в эти нехитрые манипуляции и остаются без денег. Вот, например, история из Белгорода, где пенсионерка перевела аферистам... 3,5 миллиона рублей. Женщине позвонили якобы из банка и сообщили, что кто-то пытался снять с ее счета 4,5 тысячи рублей, когда растерявшаяся белгородка ответила, что это не она, ее перевели на сотрудника «службы безопасности», а потом даже на сотрудника «полиции». Собеседники убедили пенсионерку, что помогут спасти ее деньги.

«Женщину предупредили, что она должна зарядить телефон, постоянно быть на связи и четко следовать всем инструкциям. Выполняя указания незнакомцев, женщина сняла хранившиеся в нескольких банках денежные средства и частями через разные банкоматы перевела более 3 500 000 рублей на счета злоумышленников», — говорится в сообщении пресс-службы УМВД России по Белгородской области.

Как общаться с аферистами?

Определить, что вам звонит мошенник, на самом деле очень просто: настоящий банковский служащий никогда не спросит срок действия карты, CVC-код, логин и пароль от мобильного банка, одноразовый пароль из смс-сообщения, не предложит перевести деньги на некий резервный счет.

Поэтому первое правило, когда вам позвонили и сказали о сомнительном переводе с вашего счета, — не называть собеседнику персональную информацию. «Никому не сообщайте персональные данные (паспорт, СНИЛС) или данные банковской карты (номер, срок действия, ПИН-код, смс-код безопасности). Даже если вас просит об этом сотрудник или служба безопасности банка. Банк обладает всей необходимой для совершения операций информацией, а сотрудники банка не имеют права запрашивать ее у вас», — напоминает Шумакова.

Да, не теряйте бдительность, если вам позвонили с реального телефона банка, того, что указан на карте или на официальном сайте финансового учреждения. Мошенники могут имитировать звонок с любого телефона — в интернете полно сайтов, предлагающих услугу подмены номера.

Не соглашайтесь переводить деньги со своего банковского счета или своей банковской карты на «безопасный счет» из-за сбоя или угрозы мошенничества. Запомните: самый безопасный счет для ваших денег — это ваш счет, говорит Шумакова.

Требований назвать персональную информацию и предложений перевести деньги на резервный счет достаточно для того, чтобы понять, что вы имеете дело с мошенниками. «Чувствуете, что разговор подозрительный

или нестандартный, даже если звонок с настоящего номера банка, положите трубку и сами перезвоните по номеру телефона, указанному на обратной стороне карты», — советует Шумакова.

Как вариант, над аферистами можно пошутить. Обычно мошенников ставит в тупик, когда их потенциальные жертвы признаются, что да, переводили 100 тысяч рублей в Сыктывкар. А на просьбу назвать срок действия карты, CVC-код, логин и пароль от мобильного банка можно продиктовать выдуманные данные. Злоумышленники убедятся, что вас не обмануть, и, скорее всего, больше вас беспокоить не будут.

На какие психологические крючки вас ловят финансовые мошенники

Сложная экономическая ситуация всегда способствует росту случаев финансового мошенничества. Мошенники часто используют особенности человеческой психики и поведения для достижения своей цели - это называется социальной инженерией. Портал вашифинансы.рф рассказывает об основных методах воздействия мошенников.

Быстрая помощь в решении ваших трудностей. Узнав о вашей проблеме, например, когда вам срочно нужны деньги на ремонт, вам выписали штраф или вы не можете оформить положенное пособие из-за большого количества справок, мошенник может предложить вам простое и быстрое решение, которое не потребует от вас усилий.

На вас оказывается давление. Вас пугают тем, что штраф быстро увеличится из-за пеней, пособия отменят, а проблем станет только больше. Если на вас давят, а на вопросы не отвечают или не дают понятных ответов, то стоит с подозрением относиться к такому предложению: в стрессовом состоянии принять правильное решение трудно.

Вам говорят о временных ограничениях: воспользоваться предложением можно только здесь и сейчас. Это лишает возможности как следует все обдумать.

Вам не дают возможности с кем-то посоветоваться: мошенники понимают, что в таком случае вероятность того, что вы попадется в ловушку, снижается. Именно поэтому они напоминают о срочности, о том, что это предложение действует «только для вас» и решение нужно принимать быстро.

Эксклюзивное бесплатное предложение чего-либо тоже может быть признаком мошенничества. Такие предложения нужны, чтобы усыпить бдительность и привлечь внимание к другим, платным, но якобы выгодным услугам. А фактор эксклюзивности заставляет вас чувствовать себя более значимым, из-за чего вы становитесь менее внимательным и бдительным.

Важно помнить!

Для получения любых пособий, компенсаций или других официальных выплат необходимо ваше заявление. Для этого вам, как правило, нужно самостоятельно связаться с государственными органами по телефону, через госуслуги или путём личного обращения.

Советы, которые помогут защитить себя от угроз:

- Никому не сообщайте пин-код вашей карты, ваши пароли. Храните карту и пин-код раздельно. Придумывайте сложные пароли, не используйте простые комбинации цифр, свою фамилию, даты рождения, имена детей и т.п. Используйте разные пароли для входа на разные интернет-ресурсы.

- Никому не позволяйте пользоваться вашей пластиковой картой.

- При вводе пин-кода прикрывайте клавиатуру, чтобы с камеры не была видна комбинация цифр пин-кода.

- Для оплаты покупок через Интернет заведите отдельную виртуальную карту и установите суточные лимиты для совершения покупок. Установите на банковских картах лимит выдачи средств в сутки и за одну операцию. Так мошенники не смогут снять деньги сверх установленного лимита.

- Закажите себе карту с чипом и магнитной полосой. Такая карта лучше защищена от считывания и подделки путём скимминга.
- В любой непонятной ситуации сразу звоните в свой банк по телефону, указанному на вашей карте, и уточняйте информацию.

- При утере или хищении карты срочно звоните в банк и блокируйте карту.

- Подключите услугу СМС-информирование. С ней вы будете в курсе операций по вашему счету и карте.

- Установите на компьютер и телефон лицензионную антивирусную программу.

- Пользуйтесь банкоматами, установленными в безопасных местах, оборудованных системой видеонаблюдения, охраной.

- Для продажи старых вещей через интернет-площадки используйте номер телефона, не привязанный к мобильному банкингу.

Эксперты рассказали, как обезопасить свой кошелек в отпуске

Обезопасить себя и свой кошелек от мошенников в отпуске можно, соблюдая бдительность и правила цифровой гигиены на всех этапах планирования отдыха: от покупки билетов и страховки до знакомств на пляже, рассказали РИА Новости эксперты Национального центра финансовой грамотности.

«Большинство людей начинают свои путешествия в интернете, изучая различные предложения о турах и отелях. Именно в процессе планирования отпуска можно попасть в поле зрения мошенников. Человеку, который обозначил себя поисковыми запросами, начинают поступать через рекламу или рассылку заманчивые предложения: туры по сниженным ценам, скидка на перелеты, что угодно, чтобы заставить жертву перейти по ссылкам, или открыть файл с вредоносной программой», - рассказал эксперт Дмитрий Савченко.

Он пояснил, что некоторые вредоносные программы способны считывать все вводимые логины и пароли пользователя, чтобы в дальнейшем взломать интернет-банкинг или электронные кошельки. «Невнимательный человек, может даже не заподозрить подвох и оплатить бронирование, а через некоторое время, осознать, что вместо него в оффшорные теплые страны полетели его деньги», - добавил он.

Савченко рассказал, что играя на страхах путешественников, некоторые мошенники продают фальшивую страховку для путешествий на случай COVID-19. «Когда вы покупаете страховку для путешествий, убедитесь, что покупаете полис непосредственно у лицензированной компании и всегда заранее читайте мелкий шрифт», - объяснил эксперт. Он также добавил, что избежать проблем с жильем можно, бронируя его через авторитетные сайты по аренде, которые имеют защиту потребителей, политику отмены и страховые гарантии.

«Для того чтобы обезопасить свой отдых, необходимо уведомить свой банк о поездке. Если сотрудники банка заметят, что вы начинаете совершать крупные покупки за пределами вашего обычного географического района, они смогут заблокировать вашу карту… Используйте карту с установленным низким лимитом и никогда не выпускайте свою карту из виду», - заключил он.

В свою очередь эксперт центра Елена Бобкова напомнила о мошенничествах под видом «курортных романов» или знакомств на пляже. «Если вы девушка, к вам подойдет симпатичный мужчина, если мужчина, наоборот, если семейная пара, подойдет знакомиться семья. Войдя к вам в расположение, как только вы пойдете в море, у вас пропадут все ценности из сумки, а дружелюбные знакомые исчезнут. Если вы будете внимательны к тому, что вас окружает, то сможете избежать типовых ловушек от

мошенников и успешно провести свой отпуск, вернувшись с массой положительных эмоций», - подытожила она.

27% держателей банковских карт могут стать жертвами мошенников

Многие держатели банковских карт в России сталкивались с «карточным» мошенничеством: чаще всего злоумышленники пытались по телефону узнать конфиденциальные данные карт. Несмотря на то, что большинство не потеряли деньги в результате попыток мошенничества, каждый четвертый (27%) находится в группе риска: они готовы сообщить посторонним те данные банковских карт, которые сообщать нельзя. Таковы результаты исследования Аналитического центра НАФИ.

82% россиян владеют хотя бы одной банковской картой: чаще всего это карты для получения заработной платы (50%), реже – дебетовые (32%) и кредитные карты (20%), а также социальные карты (27%).

Треть владельцев карт в России (31%) сталкивались с мошенничеством: это были попытки узнать конфиденциальные данные карты по телефону и просьбы предоставить данные для денежного перевода (например, для ложной помощи знакомым или оформления несуществующего выигрыша). Также держатели карт получали сообщения или письма с вирусами или вредоносными ссылками, сообщения о подтверждении или отмене операций по карте, которые они не совершали.

Чаще других атакам мошенников подвергались жители Москвы и Санкт-Петербурга (37% против 31% в среднем по стране), россияне в возрасте от 25 до 34 лет (35%), люди, занимающие руководящие посты (41%). Реже о попытках мошенничества сообщали люди старшего возраста (26% против 31% в среднем среди возрастных групп), при этом они в целом пользуются картами менее активно.

Подавляющее большинство держателей карт (96%) отметили, что в результате попыток мошенничества в отношении своих банковских карт не понесли финансовых потерь.

Способность распознать мошенничество свидетельствует о высоком уровне финансовой грамотности человека. Часть данных карты безопасно сообщать, например, сотруднику банка: это шестнадцатизначный номер карты, имя и фамилия держателя карты. Срок действия карты, а также трехзначный код с обратной стороны карты передавать никому нельзя.

Только 10% россиян, имеющих банковские карты, дали верные ответы на вопрос о том, какие данные карты можно сообщать сотруднику банка (номер карты, имя и фамилия держателя). Большинство россиян (63%) не готовы передавать никакие данные карт по телефону. Четверть россиян (27%) находятся в «группе риска»: они могут стать жертвами мошенников, поскольку готовы сообщить сотруднику банка по телефону данные карт, которые сообщать нельзя (срок действия, трехзначный код безопасности с обратной стороны, код из смс-сообщения).

Алексей Комисаров, директор по исследованиям Аналитического центра НАФИ:

«Довольно большая доля россиян-держателей карт, которые находятся в группе риска и готовы сообщить конфиденциальные данные своих карт, свидетельствует о недостаточном уровне просветительской работы, которая ведется банками, выпускающими карты. То, какие данные карты можно передавать, например, для денежного перевода, а какие – нет, неочевидно: банки редко сопровождают вновь выданные карты памятками с деталями.
Примечательно, что в вопросах противостояния карточному мошенничеству молодежь 18-24 лет грамотнее: 16% знают, какие данные карт можно сообщать (в среднем по возрастным группам – 10%). Однако молодежь одновременно и доверчивее: 34% готовы сообщить конфиденциальные данные (против 27% в среднем). Безопасность старшей возрастной группы обеспечивается их закрытостью: наибольшая доля тех, кто считает, что никакие данные карт передавать нельзя, достигает 72% в группе старше 60 лет (в среднем по другим возрастным группам – 63%).

Для противостояния мошенничеству банкам-эмитентам стоит активнее информировать держателей карт о том, какие данные карт сообщать можно, а какие – нет».

Что делать со старой зарплатной картой?

Зарплаты в конвертах получают лишь 10% россиян, свидетельствуют данные опроса Левада-центра. Основная часть работающих соотечественников получают деньги на зарплатные карты.

Предприятие может договориться о зарплатном проекте с новым банком, да и сотрудник может сменить место работы. А карточка останется. При этом бесплатное годовое обслуживание по ней может быть отменено: гражданин, сам того не подозревая, заплатит деньги за продукт, которым не пользуется или, что еще хуже, влезет в долги (если карта с функцией овердрафта, а деньги с нее предусмотрительно сняты). Что же делать со старой зарплатной картой?

Если вы не планируете пользоваться такой картой, ее лучше заблокировать, говорит консультант по финансовой грамотности проекта вашифинансы.рф Оксана Сидоренко. Сделать это можно в мобильном приложении или в банковском отделении, написав соответствующее заявление.

«Если на карте был нулевой баланс и банк списал деньги, которые поступили на счет, или вам отказывают закрывать карту без оплаты расходов, пишите претензию на имя руководителя финансового учреждения. Ссылайтесь на отсутствие услуги по обслуживанию счета, потому что денег на счете не было. Фактически вы в ней не нуждались», — отмечает эксперт.
Тот же порядок действий должен быть, если в счет оплаты годового обслуживания (или смс-уведомлений) были списаны деньги с кредитного лимита карточки. «Кредит — всегда волеизъявление человека, и не должно быть навязывания этой услуги со стороны банка. Напишите претензию на имя руководителя и смело защищайте свои права в суде», — подчеркивает Сидоренко.

Сложнее оспорить списание денег со счета карты, когда они там были. Напишите претензию, в которой поясните, что банк не уведомил вас надлежащим образом о таких расходах. Согласие на них вы не давали.

Банки редко признают свои ошибки и нередко отказывают клиентам в возврате средств. Искать управу на финансовую организацию придется в суде. «Ссылайтесь на закон „О защите прав потребителя“, что освобождает от оплаты госпошлины», — подсказывает эксперт.

Кстати, как напоминает эксперт Национального центра финансовой грамотности Елена Феоктистова, работник может отказаться от зарплатной карты, которую ему предлагает работодатель. «В соответствии со статьей 136 Трудового кодекса, работник вправе выбрать для себя, в каком банке открыть зарплатный счет. Работодатель не имеет право отказаться перечислять зарплату на вашу карту. Если вам удобен другой банк, получите в нем заявление о назначении счета зарплатным и передайте этот счет в бухгалтерию за 15 календарных дней до даты выплаты заработной платы», — советует Феоктистова.

Эксперт рассказал, как не стать жертвой «черного кредитора»

Оформление займа у нелегального кредитора часто выглядит безобидным и даже привлекательным для граждан, поскольку это простая процедура, не требующая подтверждения дохода, но в результате заемщик может потерять последние деньги и даже лишиться недвижимости, об этом РИА Новости рассказал президент Национальной ассоциации профессиональных коллекторских агентств (НАПКА), эксперт проекта финансовой грамотности Минфина РФ Эльман Мехтиев.

Так называемых «черных кредиторов», по словам эксперта, чаще всего можно встретить недалеко от офисов легальных компаний. «Это могут быть палатки, как в торговых рядах, так и недалеко от транспортных узлов – железнодорожных или автовокзалов. Встречались ситуации, когда в магазинах, осуществляющих прием вещей на "комиссию", предлагается получить деньги в виде займа, а в залог оставить свои документы», - рассказал он. Заём в такой «конторе» оформить очень просто, однако нелегальные кредиторы не соблюдают законодательство.

«Черные кредиторы» часто используют систему поручительства или залога, при которой даже не заключают договор, ограничиваясь получением в залог паспортов и иных документов заемщика и поручителя. «Часто в качестве залога оформляется договор купли-продажи недвижимости или транспортного средства заемщика с открытой датой. Встречались случаи, когда на физическое лицо оформляется кредитная карта, которая также остается "в залоге" и по которой "нелегалы" получают деньги от банков», - добавил Мехтиев.

По словам эксперта, в таких незаконных схемах принимают участие граждане, индивидуальные предприниматели и компании, которые не имеют права предоставлять кредиты и займы, причем их количество может быть даже сопоставимо с числом легальных кредиторов, а в ряде населенных пунктов у них даже были офисы, они расклеивали рекламу и раздавали листовки у жилых домов. Схем для афер много, так как отсутствие единого закона о защите прав потребителей финансовых услуг создают множество возможностей «отъёма денег у населения», добавил он.

«Отличить легального от нелегального кредитора на практике на сегодняшний день элементарно: все "белые" кредиторы обязаны входить в государственные реестры Банка России, а если это банк – он должен иметь лицензию. Все реестры и списки лицензированных организаций размещаются на сайте Банка России, и, если некая компания называет себя МФО, но не значится в реестре, стоит задуматься, почему это так», - считает он.

«Нелегальные кредиторы не подконтрольны в своей деятельности никому из органов, призванных стоять на защите прав потребителей финансовых услуг. Поэтому, они - "клиенты" правоохранительных органов. Вместе с тем, если вы столкнулись с такими компаниями, то рекомендуем все-таки обратиться также и в Банк России – на практике это может значительно ускорить процесс проверки, выявления фактов незаконной деятельности и санкций в отношении таких компаний», - заключил Мехтиев.