АТАКИ ТЕЛЕФОННЫХ МОШЕННИКОВ

Как их распознать и защититься

У мошенников выходных не бывает. Несмотря на то, что об их аферах постоянно рассказывают в СМИ и предупреждает полиция, преступники придумывают все новые и новые жульнические схемы. Рассмотрим наиболее распространенные способы отъема денег у граждан.

«Алло, это служба безопасности...»

Эти слова на многих уже не действуют — люди, наученные горьким опытом, уже знают, что за ними, как правило, скрываются мошенники. Поэтому сейчас потенциальной жертве звонит якобы менеджер по работе с клиентами или другой специалист банка. Он говорит, что обращается по поводу вашей заявки по кредиту, которая была оформлена через Интернет. Мошенник надеется, что собеседник возмутится: он не подавал заявку ни на какой кредит. После чего лже-менеджер сообщит, что были введены все данные жертвы: «Кому вы их передавали?». Дальше начинается запугивание, что кто-то получит деньги и повесит на вас долг. А потом вам предложат, чтобы защитить свои средства, перевести их на «специальный счет» или снять кредитные деньги самостоятельно и опять-таки отправить по якобы особым банковским реквизитам. Если жертва купится на уловку, то гарантированно потеряет свои деньги, а в придачу еще кредит возьмет, который целенаправленно попадет в лапы мошенника. Потому что никаких специальных счетов нет, и банки никогда не предлагают ничего подобного своим клиентам. На такую схему легко попасться: страшно, что кто-то повесит на вас долг. Тем более что «менеджер» торопит и не дает вам подумать. В спокойной обстановке проще

догадаться, что одной заявки в Интернете недостаточно для оформления кредита, ведь заемщик должен подтвердить свое намерение подписью. В общем, если вас спрашивают, подавали ли вы заявку на кредит, отвечайте «нет» и смело кладите трубку. Если после этого вам тревожно, позвоните в свой банк. Пусть подтвердят, что за вами нет никаких долгов.

«Идет расследование...»

В этой афере к делу подключаются «следователи», «сотрудники управлений по борьбе с экономическими преступлениями» и прочие лже-представители правоохранительных органов. Преступник звонит и невнятно представляется. Затем говорит, что был зафиксирован случай мошенничества с картой, счетами, кредитами. Злоумышленники убеждают своих жертв, что они должны поучаствовать в спецоперации правоохранительных органов по поимке преступников. Сообщают гражданам, что их помощь чрезвычайно важна, и только благодаря совместным действиям удастся задержать организованную группу. Далее предлагают совершить некие действия по переводу либо передаче денег. В большинстве случаев звонки совершаются с подменных абонентских номеров (преступники научились подделывать телефонные номера не только банков, но и полиции). В последнее время мошенники стали действовать более агрессивно, вплоть до угроз привлечения к уголовной ответственности за отказ от участия в оперативно-розыскных мероприятиях. Поэтому запомните: не существует уголовной ответственности за отказ от участия в спецоперации или разглашение данных о том, что вы узнали по телефону от не известного вам лица.

Иногда преступники выдают себя за лже-проверяющих – представителей пожарной инспекции, Роскомнадзора, прокуратуры или иных контролирующих органов. Цель та же самая – запугать какой-то мифической проверкой и выманить ваши денежки.

«Минуту назад вам звонили мошенники...»

Здесь осуществляется обман в несколько ходов. Сначала потенциальной жертве звонит очевидный мошенник, которого легко проигнорировать. А затем с ней связывается лжесотрудник банка или поддельный полицейский. Он говорит, что зафиксировал звонок злоумышленника, и с этим надо разобраться. В процессе он попросит назвать данные карты, или перевести деньги на специальные счета, или оформить кредит — возможны варианты.

В реальной жизни описанная ситуация практически невозможна, ведь для этого настоящему оперативнику пришлось бы сутки напролет прослушивать ваш телефон, чтобы засечь потенциального преступника. Но даже если б это было так, то мошенник у вас ничего не похитил: чем же вы можете быть полезны для следствия? Так что, не вдаваясь в долгие разговоры, просто кладите трубку.

Как понять: звонят из настоящего банка или это преступник?

Сотрудники банка иногда действительно могут позвонить, чтобы задать вопросы о качестве обслуживания и предложить новые акции или условия оформления кредита. А если вы оставляли заявку на кредит, то с вами обязательно свяжется специалист из банка: он может поинтересоваться размером ваших доходов или стажем работы. Но НИКОГДА настоящий сотрудник банка не станет интересоваться сведениями о карте и тем более CVV-номером на ее обратной стороне.

Особо стоит обратить внимание на звонок сотрудника службы безопасности банка, так как часто именно под таким предлогом звонят мошенники. Настоящий сотрудник банка будет звонить только после того, как карту клиента заблокировали. Он спросит ФИО, место прописки, дату рождения или кодовое слово (которое содержится в дого-

воре с банком). Однако, если вы не блокировали свою карту, «сотрудник службы безопасности», скорее всего, является мошенником.

Правильная реакция после получения сомнительного звонка только одна: позвонить в банк самому и прояснить ситуацию.

Зачем аферисты подделывают чужие голоса

В 2018 году российские банки начали собирать биометрические данные клиентов — с их помощью граждане могут обращаться в финансовые организации без личного присутствия, по телефону — кредитные учреждения идентифицируют их по цифровому «отпечатку» голоса. Собирать биометрические данные россиян начали и аферисты: они звонят людям, задавая невинные вопросы, и просят отвечать на них «да» или «нет». Затем они собирают данные о ваших контактах. После этого с помощью специальных приложений, которые позволяют изменить голос, набирают номер вашего знакомого или родственника и вашим голосом просят перевести деньги на определенный счет. Предлогом может стать «срочная помощь на лечение» или «на выплату долга» и так далее.

На эту мошенническую уловку не раз попадались даже очень крупные предприниматели. К примеру, в январе прошлого года в один из банков позвонил мужчина, представившийся руководителем крупной компании, и сообщил, что его фирма готова заключить сделку, но сумму нужно перевести на новые счета. Сотрудник банка согласился, ведь недавно он общался с этим клиентом, узнал его и был уверен, что и сейчас разговаривает с ним — голос тот же... В итоге деньги со счета реального клиента, чей голос подделали мошенники, разлетелись по разным счетам по всему миру.

Для того, чтобы не стать жертвой таких мошенников, нужно в первую очередь взять за правило следить за своей речью

в момент разговора с возможным представителем банка. Вместо ответа «да» на телефонный звонок скажите «слушаю» или «алло». Старайтесь уходить от прямых ответов на вопросы, пока в ходе разговора не услышите достаточно конкретики. Помимо этого в разговоре с неопределенными лицами по телефону используйте вводные слова – «так сказать», «возможно» и другие: они сбивают алгоритмы злоумышленников. Еще один вариант защиты — во время разговора тянуть гласные звуки.

Получается, нельзя верить никакому звонку? Нельзя, если звонок необычный и за ним следует странная (не свойственная для позвонившего) или не совсем законная просьба. Современная техника позволяет подделывать голос и подменять номер телефона, с которого идет вызов.

«Поздравляем: вам положена выплата!»

Чаще всего с таким «радостным сообщением» звонит якобы сотрудник Пенсионного фонда и объявляет: «Вам положена выплата, но потерялся номер счета для зачисления денег. Сообщите, пожалуйста, данные своей карты». Если вы купились на эту уловку, а потом вдруг опомнились, срочно звоните в банк, чтобы там успели заблокировать карту, иначе деньги исчезнут довольно быстро. Другие уловки этого типа — выигрыш в лотерею, для получения которого нужно «заплатить налог», или письмо о подарке, «доставку которого требуется оплатить». А как только деньги перечисляются, благожелатели исчезают. Мошенническая новинка этого года – сообщение о «денежной премии за вакцинацию».

Если ваши деньги украдены, а вы при этом не сообщали никаких данных своей карты, необходимо обратиться в свой банк и в полицию. По закону банк должен вернуть похищенные средства на счет клиента, если тот не нарушал договор об обслуживании: в частности, не сообщал посто-

ронним людям информацию, которая могла способствовать хищению, например, данные банковской карты и пароли из СМС. Поэтому, чтобы защитить свои деньги, ни под каким предлогом не сообщайте эти данные посторонним людям, кем бы они ни представлялись — сотрудниками банка или правоохранительных органов. Пенсионерам банки рекомендуют чаще советоваться с детьми и друзьями. А чтобы совместное решение принимать было проще, можно оформить в банке «сервис второй руки». То есть по просьбе клиента-пенсионера назначить ему помощника, имеющего право проверить и отклонить нетипичную финансовую операцию.

«Поможем вернуть украденное!»

Отдельная категория «помощников» — лже-юристы, предлагающие вернуть украденное мошенниками. По телефону они обещают бесплатную консультацию и, войдя в доверие, подсовывают платный договор, «гарантирующий стопроцентный результат». Затем по шаблону готовятся документы для подачи в правоохранительные органы, но никакой юридической пользы они не приносят.

Как отличить шарлатанов от профессионалов? У консультантов, имитирующих правовую помощь, обычно нет «лица», такие юридические фирмы-однодневки максимально обезличены. Если вы позвоните им по телефону, то не услышите фамилий сотрудников, которые представляются и говорят от имени фирмы. Часто у них нет даже постоянного офиса с адресом: они могут создать сайт в Интернете и отвечать на вопросы, не выходя на прямую связь с клиентом, и таким же способом получать от него деньги. Либо давать свои консультации, сняв небольшую комнату где-нибудь в крупном торговом центре без конкретного адреса и телефона. Поэтому не спешите оплачивать договор после бесплатной консультации: сначала ознакомьтесь с историей фирмы, поинтересуйтесь, сколько лет

работает юрист, предлагающий вам помощь, ознакомьтесь с его документами. Потребуйте назвать ИНН и попросите знакомых, имеющих доступ в Интернет, проверить, зарегистрирована ли фирма в открытых налоговых базах (по номеру ИНН это сделать легко). Если хоть что-то насторожило, проигнорируйте предложение и найдите других юристов.

Интернет-ловушки

Сегодня многие пенсионеры научились не только звонить с помощью современных телефонов, но и писать сообщения, пересылать фото в специальных приложениях. С их помощью можно удобно общаться и обмениваться информацией в любое время суток, не переживая, что нарушишь чей-то покой или отвлечешь человека от дел. И, конечно, аферисты не упустили возможности использовать телефонные приложения в своих схемах. К примеру, они от имени известных людей (артистов, спортсменов) рассылают телефонные сообщения о временных финансовых трудностях или проблемах со здоровьем знаменитостей или призывают позаботиться об их больных детях. Все это выглядит весьма правдоподобно, имитирует манеру общения популярных людей, сопровождается многочисленными фотографиями тех, кто попал в сложное положение. Естественно, к просьбе о помощи прилагается номер счета, куда просят перечислить «хотя бы один рубль». Но если вы действительно готовы помочь знаменитому человеку, попавшему в беду, зайдите в банк и переведите деньги на счет благотворительного фонда, которому доверяете: так они точно дойдут до адресата.

Еще одна «удочка», на которую часто попадаются пользователи современных телефонов, – это увлечение рекламой. Получив в СМС-сообщении по телефону предложение купить что-то с хорошей скидкой и не выходя из дома, многие забывают о том, что за «выгодной покупкой» может

стоять обычная афера. Мошенники даже предлагают зайти на их сайт в Интернете и ознакомиться с другими «выгодными акциями». Многие из них отвечают на телефонные звонки и подтверждают наличие скидок: «Только надо забронировать ваш товар и внести за него 10% от стоимости».

В результате жертвы рекламы вносят на счет мошенников небольшую предоплату и ждут, когда им привезут товар, готовясь расплатиться за него полностью. Однако в результате ничего не получают. Статистика обращений граждан в полицию в течение двух лет пандемии показывает, что мошенники имитируют продажу все новых вещей и услуг. Так, у знаменитого АвтоВАЗа найдено 188 фальшивых сайтов, откуда преступники выманивали деньги у людей, желающих купить автомобиль с хорошей скидкой. За минувшее лето в 10 раз увеличилось число поддельных интернет-страниц, где продаются дорогие билеты на спектакли театров и концерты. Поэтому, если вы, прельстившись рекламой, очень хотите сделать выгодную покупку, не торопитесь вносить за нее предоплату. Сначала либо попросите опытного пользователя Интернета проверить, не является ли сайт и сообщение подделкой, либо сами поезжайте в магазин и совершите покупку через кассу, где вам выдадут чек. Это, хоть и займет время, но точно сохранит деньги. Кроме того, чек является гарантией и возможностью вернуть товар, если он вам не подойдет.

Олеся КАЛЬНИЦКАЯ,
юрист, адвокат.