# Телефон недоверия

Антология мошеннических схем, использующих СМС и мобильные телефоны

Текст:
Наталья Югринова

**По статистике Банка России, почти 78% всех финансовых мошенничеств в 2018 году осуществлялось через интернет и мобильные устройства. Чтобы выманить деньги у доверчивых сограждан, преступники обещают им вклады под огромные проценты, притворяются сотрудниками банка или представителями госорганов, присылают СМС с вредоносными ссылками — словом, подходят к делу изобретательно. Как распознать мошенника и можно ли вернуть деньги, если вас всё же обманули?**

Мобильные телефоны давно перестали быть простым средством голосовой связи и прочно заняли место в системе платёжных инструментов. К ним привязаны банковские карты, на них приходят одноразовые коды с подтверждениями интернет-платежей, а за многие услуги и сервисы можно расплатиться прямо с баланса смартфона. Там, где есть денежные транзакции, появляются и мошенники. По данным ЦБ РФ, в 2018 году объём несанкционированных операций, совершённых с использованием платёжных карт, вырос на 44% — правда, столь резкий

рост аналитики связывают не с увеличившейся активностью мошенников, а с повышением выявляемости подобных случаев. Всего у россиян в прошлом году с банковских карт было похищено более 1,3 млрд рублей, в восьми из десяти случаев — при помощи телефонных звонков, через СМС или онлайн.

Как правило, информация об очередном виде мошенничества по телефону распространяется довольно быстро. Жертвы и те, кто избежал обмана, публикуют свои истории в социальных сетях, финансовые институты выпускают официальные предупреждения и просьбы быть бдительными. Однако подготовить себя к абсолютно всем ситуациям, в которых вы можете столкнуться с телефонным аферистом, невозможно. Преступники постоянно изобретают новые схемы и варьируют сценарии в зависимости от возраста и степени доверчивости собеседника. Они могут знать ваши личные данные: имя, фамилию, дату рождения, адрес проживания и другие сведения нетрудно получить из открытых источников или различных платных баз данных. Иногда в аферу вовлечены несколько человек, каждый из которых играет свою роль и звонит с нового телефонного номера, подтверждая слова предыдущего звонящего. В зависимости от целей, всех телефонных мошенников можно разделить на три группы.

**1. «Вымогатели денег»** с помощью пустых обещаний, угроз или шантажа пытаются вынудить вас совершить денежный перевод в их пользу.

**2. «Похитители данных»** стараются выяснить данные вашей банковской карты, ПИН-код, CVV-код.

**3. «Мастера скрытых продаж»** заставляют вас выполнить какое-то действие (совершить ответный звонок, послать ответное СМС, набрать комбинацию цифр на телефоне и т. д.), которое подпишет вас на мошеннический сервис.

С каким бы из типов этих мошенников вы ни столкнулись, стоит принять к сведению совет, который даётся в методическом пособии «Бабушки против мошенников» (подготовлено и издано на грант Президента РФ в 2019 году). «Телефонное мошенничество, — пишут авторы, — возможно только тогда, когда абонент на связи. Если он положил трубку и не подходит больше к этому номеру телефона, скорее всего, мошенники не будут именно до него часами дозваниваться. Как правило, работают они широким охватом, обзванивая все подряд номера. Если из 100 попыток обмануть по телефону успешными оказались 10, они всё равно окажутся в выигрыше — получив деньги и при этом совсем ничего не сделав и практически ничего не потратив. Поэтому, если поступил непонятный, странный, тревожный звонок с незнакомого номера, следует немедленно положить трубку, а потом собраться с мыслями и успокоиться, а возможно, и позвонить родным».

Вот несколько реальных ситуаций, которые иллюстрируют, как могут действовать мошенники — и как им следует противостоять.

## Случай 1
## «Вашу карту нужно заблокировать»

***Что происходит.*** Вам звонят с телефона, который определяется как официальный номер банка или похожий на него (например, для Сбербанка это номера 900 и +7 (495) 500-55-50), и предупреждают о попытке несанкционированного списания средств с карты. При необходимости называют ваши паспортные данные, последние транзакции и даже остаток по счёту. Собеседник предлагает заблокировать вашу карту, а деньги временно перевести на специальный «защищённый» счёт. Для этого вам нужно всего лишь назвать «оператору» код, который придёт в СМС-сообщении от банка. Полученный код злоумышленники используют, чтобы поменять пароль доступа к интернет-банку владель-

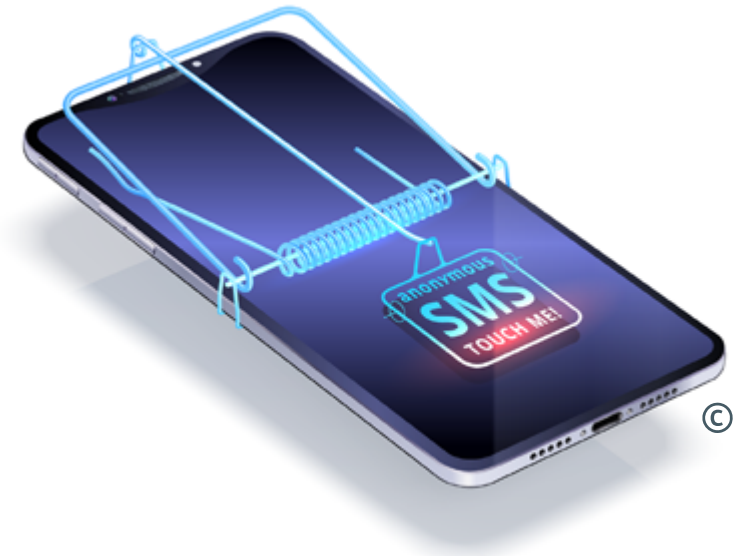
ца карты, а также привязанный к нему номер телефона. После этого они опустошат счёт жертвы.

***Что делать?*** В конце января 2019 года с подобной проблемой столкнулись Сбербанк, Юникредит-банк и Райффайзенбанк. Банки выпустили официальные предостережения и напомнили клиентам, что ни в коем случае нельзя сообщать по телефону никакие данные о своих платёжных картах, CVV-коды или одноразовые коды 3D-Secure, — даже тому, кто звонит с номеров банка и представляется его сотрудником. Единственный вариант удостовериться, что вам действительно позвонили из банка, — положить трубку, найти телефон контактного центра (он напечатан на обороте карты) и самим перезвонить по нему.

## Случай 2
## «Откройте вклад под 20% годовых»

***Что происходит.*** Вы получаете СМС с заманчивым предложением: открыть вклад под процент гораздо выше среднерыночного или получить дешёвый кредит. Ставка привлекательная, имя банка-отправителя — известное, к тому же действовать предлагается срочно, ведь выгодная акция очень скоро заканчивается. Вы звоните по указанному номеру (или отправляете через СМС согласие) и выясняете детали. Вам тут же сообщают, что в вашем регионе филиала этого банка нет, поэтому он действует через партнёра, на «сберегательный» счёт которого и нужно перевести ваши средства. В случае кредита схема несколько иная: чтобы его получить, нужно купить страховку — удобнее всего простым перечислением на карточку частного лица. Разумеется, как только вы переводите деньги, мошенники перестают выходить на связь.

***Что делать?*** В интервью газете «АиФ» начальник Главного управления ЦБ РФ по Центральному федеральному округу **Надежда Иванова** объясняет, что мошенники часто действуют от имени ликвидированных или лишённых лицензии банков. Иногда для пущей убедительности они даже создают простенький сайт, на котором размещают якобы выгодные условия своих финансовых продуктов. Эксперт советует обязательно проверять в справочнике кредитных организаций на сайте Центробанка РФ, работает ли ещё этот банк. А если работает — узнать его официальный сайт и телефон, позвонить и расспросить о процентных ставках и необходимых документах. Заодно стоит раз и навсегда запомнить: ни один банк не будет предлагать вам условия, которые сильно отличаются от средних на рынке. Иначе он просто не сможет быть финансово устойчивым.




## Случай 3
## «Здравствуйте, я по объявлению»

***Что происходит.*** Вы недавно выставили на продажу какую-либо вещь на онлайн-сервис с такого рода объявлениями («Авито», «Юла», «Из рук в руки» и т. п.). Через час–два вам звонит покупатель и объясняет, что товар ему очень нужен, но он не в городе — поэтому готов прямо сейчас отправить деньги вам на карту, а за покупкой завтра заедет друг (в некоторых вариантах — курьер службы экспресс-доставки). Вы радуетесь столь быстрому закрытию сделки и немедленно соглашаетесь. Покупатель узнаёт у вас номер карты и со словами «Ждите оплаты» кладёт трубку. Далее вам звонит другой человек, представляется сотрудником банка и спрашивает, ожидаете ли вы денежный перевод на такую-то сумму (она совпадает с той, которую вы сообщили покупателю). После сверки основных данных он отправляет вам в СМС код, который вы должны переслать покупателю, — только тогда перевод можно будет осуществить. Вы действуете согласно полученной инструкции. Только никаких денег на ваш счёт не поступает — напротив, выясняется, что мошенники списали с него крупную сумму, подтвердив операцию через код, который вы сами им и отправили.

***Что делать?*** Стоит сразу обратиться по официальному телефону в банк и объяснить, что вы, скорее всего, стали жертвой мошенников. Банк может успеть заблоки-

ровать подозрительную операцию и «заморозить» движение списанных с вашей карты средств. В любом случае помните: кто угодно может пополнить вашу карту, зная один лишь её номер. Никаких кодов подтверждения вам сообщать отправителю не требуется.

## Случай 4
## «Прислали деньги по ошибке»

***Что происходит.*** Консультант по финансовой грамотности проекта «Вашифинансы.рф» **Елена Лобова** поделилась такой историей. Однажды в час ночи с неизвестного номера она получила СМС: «Поступил платёж 300 руб. Спасибо, что пользуетесь услугами МТС». Через несколько минут с другого номера пришло ещё одно сообщение: мол, отправитель спохватился, что послал деньги не туда, и попросил вернуть их, причём на третий номер. Такие сообщения часто специально присылают ночью: человека спросонья легче обмануть.

***Что делать?*** Прежде всего Елена проверила свой баланс и увидела, что никакого ошибочного пополнения счёта не было. Если кто-то действительно ошибочно переведёт вам деньги, вы получите сообщение с официального короткого номера оператора, а не со случайного незнакомого телефона. Лучше всего позвонить оператору на горячую линию и продиктовать номера мошенников: если после проверки факты подтвердятся, оператор может заблокировать злоумышленников.

## Случай 5
## «Получите вашу компенсацию»

***Что происходит.*** Пожилому человеку звонят с незнакомого номера, представляются следователями (прокурорами, судьями, адвокатами и т. д.) и объявляют, что ему положена компенсация. Пенсионер якобы стал жертвой мошенничества — купил несколько лет назад биологически активные добавки, а следствие установило, что лекарства не имеют заявленного эффекта. Теперь он является потерпевшим по уголовному делу и может рассчитывать на крупную денежную компенсацию — в несколько сотен тысяч рублей. Только для того, чтобы получить её, нужно сначала оплатить комиссию в 5% от этой суммы. Если человек соглашается и выполняет условие, мошенник понимает, что поймал его «на крючок». Он начинает вымогать дальнейшие платежи под предлогом необходимости заплатить налог, страховку

Телефонное и СМС-мошенничество подпадают под статью 159 Уголовного кодекса РФ. Наказание по ней предусматривает штраф в размере до 1 млн рублей (в зависимости от размера ущерба), общественные работы или лишение свободы на срок до 5 лет.

и прочее — при этом сумма фантомной компенсации тоже растёт. В 2018 году 75-летняя жительница Петропавловска-Камчатского, например, отдала таким образом мошенникам более 1,3 млн рублей.

***Что делать?*** Объектом мошенничества по схеме покупателей БАД (иногда компенсацию обещают за «сгоревшие» вклады в МММ и других финансовых пирамидах 1990-х) становятся, как правило, пожилые и тяжелобольные люди. Их подкупает то, что звонящий обращается к ним по имени и фамилии и оперирует фактами: пенсионер действительно покупал лекарства, о которых идёт речь. Очевидно, что мошенники получили доступ к базам данных с перечнем граждан, когда-то приобретавших БАД, их телефонами и паспортными сведениями. Лучший способ предохраниться от такого вида мошенничества — при попытке подобного контакта самому перезвонить в официальный орган и узнать, действительно ли вам полагается компенсация.

## Случай 6
## «Мама, я попал в аварию»

***Что происходит.*** Раздаётся телефонный звонок, и мужской дрожащий голос говорит: «Мама, я попал в аварию, нужно

30 тысяч, за деньгами заедут». Мошеннику может повезти, если он действительно попадёт на чью-то легковерную мать, сын которой теоретически мог угодить в ДТП. У женщины не возникает вопросов, почему голос сына звучит по-другому, почему звонит с чужого номера и зачем ему деньги. Она сразу бежит снимать сбережения. И только после того, как отдаст деньги преступникам, может позвонить настоящему сыну — чтобы выяснить, что он в абсолютном порядке и ведать не ведает ни о какой аварии.

***Что делать?*** Правоохранительные органы советуют всегда проверять информацию о любых несчастных случаях, якобы произошедших с вашими родственниками, прежде чем отдавать деньги незнакомым людям. Сделать это следует, позвонив дежурному офицеру по номерам 02 или 102, а также связавшись с самим родственником.

## Случай 7
## «У вас есть неоплаченный штраф»

***Что происходит.*** Приходит СМС с напоминанием о том, что вам необходимо оплатить штраф ГИБДД или задолженность по коммунальным услугам. В сообщении указана ссылка на сайт, через который можно провести платёж, либо указан короткий номер, на который можно отправить СМС для его оплаты. Пользователь переходит по фишинговой ссылке, вводит данные своей карты, деньги с его счёта списываются — но попадают совсем не на счёт искомой организации, а в карман мошенникам. Ещё один распространённый вариант: при нажатии на ссылку на смартфон загружается вирус, который может украсть все данные вашей карты.

***Что делать?*** Правила просты: установить на мобильное устройство антивирусную программу, никогда не переходить по ссылкам из СМС и проверять все штрафы и задолженности перед бюджетом на официальных сайтах государственных организаций.

## Случай 8
## «Я поцарапала вашу машину»

***Что происходит.*** Человеку с незнакомого номера приходит текстовое сообщение, в котором отправитель (обычно девушка) пишет, что якобы поцарапала его машину. Такие рассылки могут отправлять как тем водителям, которые оставляют свои номера на лобовом стекле для экстренной связи, так и «наобум» — даже тем, у кого нет автомобиля. Если жертва перезванивает на указанный номер, то со счёта списывают крупную сумму денег — номер оказывается платным, и стоимость минуты общения на нём крайне велика.

***Что делать?*** Никогда не перезванивать на незнакомые номера: если что, всегда можно написать ответное сообщение в WhatsApp или других мессенджерах, это бесплатно. Кроме того, прежде чем реагировать на подобные сообщения, стоит убедиться, что вашему автомобилю действительно нанесён ущерб. Если вы поняли, что вас пытаются обмануть, сообщите номер мошенника на горячую линию своего мобильного оператора.

Общее правило для пострадавших от мошенников сводится к тому, что нужно заблокировать карту, если с неё списывают деньги без вашего ведома, опротестовать подозрительные операции в отделении банка и обратиться с заявлением в полицию. Впрочем, даже если вы выполните все эти условия, деньги могут так и не вернуться. Как указывает образовательный ресурс Fincult.ru, если банк докажет, что вы нарушили правила использования карты, то возмещать средства он не обязан. Под такие нарушения подпадает разглашение третьим лицам реквизитов своей карты, её ПИН-кода и CVV-кода. В общем и целом случаи возврата денег регулирует Федеральный закон «О национальной платёжной системе» — однако он не помогает в случае, если мошенники опустошили ваш электронный кошелёк или другие неперсонифицированные платёжные средства.

Сами банки, в свою очередь, постоянно работают над совершенствованием своей системы безопасности. В частности, в апреле 2019 года Банк России заявил, что соберёт с финансовых организаций телефоны их клиентов, звонящих на автоинформатор с целью узнать остаток на счёте. Это один из способов, которыми мошенники могут получить конфиденциальную информацию, а затем использовать её в своих интересах, звоня потенциальной жертве. Ведение таких списков, по задумке регулятора, может отсечь часть мошеннических звонков. Но в первую очередь, конечно, лучше полагаться на собственную бдительность.