# **ПАМЯТКА**

# **КАК НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ**

Мошенничество с использованием сотовой связи и сети Интернет приобретает все большие масштабы. Мошенники, пользуясь достижениями технического прогресса, имеют возможность действовать анонимно, «охватывать» большое количество абонентов телекоммуникационных сетей и обогащаться, пользуясь доверчивостью и невнимательностью граждан.

Раскрыть преступления данной категории весьма сложно, в связи с тем, что мошенники работают удаленно, впоследствии отключают телефоны, убирают адреса и т.д.

Чтобы не стать жертвой кибер-мошенников, необходимо знать о способах обмана, которые используются для совершения хищения денежных средств.

Наиболее распространенными способами телефонного мошенничества являются следующие:

1. **Сообщение специалиста службы безопасности банка о несанкционированном переводе денежных средств, доступе к онлайн-банку, оформленном без согласия кредите.**

Вам звонят с незнакомого номера (зачастую с кодом другого региона). Мошенник представляется специалистом службы безопасности банка, называет ваши данные (вплоть до номеров банковских счетов и сумм денежных средств на них) и информирует вас о том, что был осуществлен несанкционированный перевод денежных средств либо попытка взлома онлайн-банкинга. В дальнейшем, «для возврата и защиты денежных средств» жертве предлагается пообщаться с другим «специалистом банка» и выполнить предложенный им порядок действий (сообщить коды из смс-сообщений, войти в приложение онлайн-банк, совершить перевод денежных средств с одного счета на другой). Выполнение предложенных мошенниками действий позволит им получить доступ к банковскому счету и совершить хищение денежных средств.

Помимо несанкционированных переводов, доверчивым гражданам могут сообщить об оформленном на их имя кредите и предложить аннулировать заявку на кредит либо оформить страховку с целью сохранения денежных средств от списания в счет погашения «мифического кредита». Далее также предлагается совершить ряд действий с сообщением кодов, данных банковской карты и т.п., что повлечет хищение денег со счета либо оформление уже реального кредита на имя жертвы.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ: Не выполняйте никаких действий, предложенных по телефону псевдоспециалистами банка, не сообщайте данные своей банковской карты и коды, направленные вам посредством смс-сообщений, не совершайте переводов денежных средств со счета на счет по требованию звонящего. Не ленитесь самостоятельно позвонить в банк по номеру телефона, указанному на банковской карте, либо лично посетить офис, в котором у вас открыты счета и подключены онлайн-сервисы, и выяснить информацию о состоянии банковского счета.

1. **Требование выкупа**

Вам звонят с незнакомого номера. Мошенник представляется родственником или знакомым и сообщает, что задержан сотрудниками полиции и обвинён в совершении того или иного преступления. Далее в разговор вступает якобы сотрудник полиции, который заверяет, что проблема решаема, но для этого необходима определенная сумма денег, которую следует перевести по указанным им реквизитам. При этом мошенники стараются запугать жертву, не дать ей опомниться, поэтому ведут непрерывный разговор с ней вплоть до получения денег.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ: Первое и самое главное правило – прервать разговор и перезвонить тому, о ком идёт речь. Если телефон отключён, постарайтесь связаться с его коллегами, друзьями и родственниками для уточнения информации. Следует понимать: если незнакомый человек звонит вам и требует денежную сумму – это мошенник.

Беседуя с близким родственником или знакомым, попавшим якобы в неприятную ситуацию, следует задать уточняющие вопросы, ответы на которые знаете вы оба.

Если вы разговариваете якобы с представителем правоохранительных органов, поинтересуйтесь из какого он отделения полиции. После звонка следует набрать «02», узнать номер дежурной части данного отделения и выяснить, действительно ли родственник или знакомый доставлен туда.

Следует знать, что требование взятки является преступлением.

1. **SMS-просьба о помощи**

Абонент получает на мобильный телефон сообщение: «У меня проблемы, кинь 900 рублей на этот номер. Мне не звони, перезвоню сам». Нередко добавляется обращение «мама», «друг» или другие.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ: Пожилым людям, детям и подросткам следует объяснить, что на SMS с незнакомых номеров реагировать нельзя, это могут быть мошенники.

1. **Телефонный номер-грабитель**

Вам приходит SMS с просьбой перезвонить на указанный номер мобильного телефона. Просьба может быть обоснована любой причиной – помощь другу, изменение тарифов связи, проблемы со связью или с вашей банковской картой и так далее. После того как вы перезваниваете, вас долго держат на линии. Когда это надоедает, вы отключаетесь – и оказывается, что с вашего счёта списаны крупные суммы денег.

Существуют сервисы с платным звонком. Реклама таких сервисов всегда информирует о том, что звонок платный. Мошенники же регистрируют такой сервис и распространяют номер без предупреждения о снятии платы за звонок.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ: Не звонить по незнакомым номерам. Это единственный способ обезопасить себя от телефонных мошенников.

1. **Телефонные вирусы.**

Очень часто используется форма мошенничества с использованием телефонных вирусов. На телефон абонента приходит сообщение следующего вида: «Вам пришло MMS-сообщение. Для получения пройдите по ссылке…». При переходе по указанному адресу на телефон скачивается вирус и происходит списание денежных средств с вашего счета.

Другой вид мошенничества выглядит так: при заказе какой-либо услуги через якобы мобильного оператора или при скачивании мобильного контента абоненту приходит предупреждение вида: «Вы собираетесь отправить сообщение на короткий номер …, для подтверждения операции отправьте сообщение с цифрой 1, для отмены с цифрой 0». При отправке подтверждения, со счета абонента списываются денежные средства.

КАК ДЕЙСТВОВАТЬ В ТАКОЙ СИТУАЦИИ: Не следует переходить по указанным в сообщениях ссылкам или звонить по номеру, с которого отправлено SMS – вполне возможно, что в этом случае с вашего телефона будет автоматически снята крупная сумма.

**6. Выигрыш в лотерее.**

На ваш мобильный телефон звонит якобы ведущий популярной радиостанции и поздравляет с крупным выигрышем в лотерее, организованной радиостанцией и оператором мобильной связи. Это может быть телефон, ноутбук, крупная сумма денег или даже автомобиль. Чтобы получить приз, необходимо оплатить определенную денежную сумму либо выполнить ряд действий (назвать полные данные банковской карты для зачисления выигрыша, набрать определённую комбинацию цифр, сообщить коды из смс-сообщений и т.п.).

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ: Если вам сообщили о проведении лотереи только в момент «выигрыша», и при этом ранее вы не заполняли заявку на участие в ней и никак не подтверждали свое участие в розыгрыше, то вас пытаются обмануть. Оформление документов и участие в таких лотереях никогда не проводится только по телефону и Интернету.

1. **Простой код от оператора связи.**

Вам поступает звонок либо приходит SMS-сообщение якобы от сотрудника службы технической поддержки вашего оператора мобильной связи. Обоснования этого звонка или SMS могут быть разными: предложение подключить новую эксклюзивную услугу; перерегистрация во избежание отключения связи из-за технического сбоя; улучшение качества связи;  предложение принять участие в акции от вашего сотового оператора; защита от СПАМ-рассылки и др.

Вам предлагается набрать под диктовку код или сообщение SMS, которое подключит новую услугу, улучшит качество связи и т.п.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ:  Не спешите выполнять то, о чем просит звонящий. Перезвоните своему мобильному оператору для уточнения условий.

**8. Доступ к SMS и звонкам.**

В Интернете или прессе публикуется объявление, в котором вам предлагается изучить содержание SMS-сообщений и список входящих и исходящих звонков интересующего Вас абонента. Для этого необходимо отправить сообщение определенной стоимостью на указанный короткий номер и вписать в предлагаемую форму номер телефона абонента. После того как вы отправите SMS, с вашего счета списывается сумма намного больше той, что была указана мошенниками.

КАК ПОСТУПАТЬ В ТАКОЙ СИТУАЦИИ: помните, что предложение о предоставлении данной услуги является мошенничеством, так как она может оказываться исключительно операторами сотовой связи и в установленном законом порядке.