

Как не стать жертвой телефонных мошенников

За последний год количество звонков с неизвестных номеров выросло в геометрической прогрессии. Часто неискушенный человек не в силах распознать природу каждого из них, но в основном это либо агрессивный спам, либо попытка мошенничества. Телефонные аферисты идут на все новые уловки: например, они стали чаще ссылаться на Центробанк России, который якобы одобрил заявку на кредит. Такого не может быть по определению: регулятор такими вещами не занимается.

Согласно статистике ЦБ, объем денежных потерь российских граждан от телефонного мошенничества в 2022 году составил 14,2 млрд рублей, а **случаев хищений средств с банковских счетов набралось 877 тысяч**.

При этом из года в год доля возврата населению их средств становится все более символической. То есть кража означает безвозвратную потерю.

В 2022-м банки вернули клиентам 618,4 млн рублей, или 4,4% от всего объема (в 2021 году показатель составил 6,8% или 920 млн рублей). Такой низкий уровень возмещения связан с **активным использованием методов социальной инженерии**, когда люди **добровольно переводят третьим лицам** свои деньги или раскрывают банковские данные.

Средняя сумма одной мошеннической операции выросла на 29,8%, до 15,3 тысяч рублей. Сегодня такого рода деятельность фиксируется в основном **в сфере дистанционных банковских сервисов — мобильном и интернет-банкинге** (общий размер потерь здесь – 9,3 млрд рублей).

Центробанк России в 2022-м году **инициировал блокировку более 756 тысяч мошеннических телефонных номеров** — в четыре с лишним раза больше, чем годом ранее. Среди других мер противодействия регулятор рекомендует гражданам **устанавливать самозапрет на выдачу кредитов, а также на онлайн-операции, либо ограничивать их параметры** — максимальную сумму для одной транзакции или лимит на определенный период времени.

На сайте Центробанка перечислен **список типичных мошеннических схем**. В их числе сценарии, когда телефонные злоумышленники: представляются сотрудниками ЦБ (или даже ФСБ) и сообщают о «сомнительных операциях» по счету или карте, предлагая сверить банковские данные; просят перевести средства на специальный «защищенный» счет ЦБ; убеждают оформить кредит; обещают помочь с компенсацией похищенных денег — для этого клиент должен заполнить форму с личными и финансовыми данными.

Существует единственно верный и эффективный метод противодействия: если вам позвонил «сотрудник» банка или полиции и из «соображений безопасности» попросил поделиться, скажем, секретным ПИН-кодом, тут же кладите трубку. Не стоит искушать судьбу, ввязываться в разговор. Лучше свяжитесь чуть позже со своей кредитной организацией и поинтересуйтесь, в чем дело. Сам банк не будет вас беспокоить, только если вы не просрочили кредит на большую сумму. Это ведь азбучная истина; странно, что жертвами такого рода афер ежегодно становятся десятки, сотни тысяч людей.

Суть того, что делают телефонные мошенники, не меняется: им надо найти потенциальную, поддающуюся психологической обработке жертву, вытянуть данные по карте, наконец, списать деньги и перевести на свой счет. А вот легенда и конкретные способы всякий раз другие: то это просьба прислать QR-код для отмены «несанкционированной операции», то авария, то одобренный кредит, то крупный выигрыш в лотерею.

Первая рекомендация — **ничего сообщать им не нужно**: вы либо сразу прекращаете разговор, либо ограничиваетесь фразой: «Спасибо, в ваших услугах не нуждаюсь». Надо четко понимать, что эти люди используют определенные техники внушения.

Во-вторых, по возможности **не держите крупных сумм на дебетовой карте**. Разве что на депозите.

В-третьих, если вы хотите застраховать свои средства, то (в соответствии со статьей 9 федерального закона «О национальной платежной системе») вам следует заключить с банком договор, согласно которому вы будете **получать СМС-оповещения о каждой транзакции**. Стоит такая услуга совсем недорого. Увидев, что произошло несанкционированное списание денег с карты, **вы должны в течение суток известить об этом банк**. Тот, в свою очередь, проведет собственное расследование, и, если факт мошенничества подтвердится, сумму вам восстановят в прежнем объеме.

Центробанк России запустил обучающий сайт для борьбы с финансовыми пирамидами и обманом в сети. Этот **ресурс под названием «Рублерост»** имитирует различные мошеннические проекты. На нем, как заявляет регулятор, собраны наиболее часто используемые уловки, ознакомление с которыми поможет не попасться на крючок аферистов, обещающих высокий доход при минимальных усилиях.

(По материалам сайта Центробанка России и публикаций российских средств массовой информации)

Май 2023