**«Ваша карта заблокирована» и другие популярные схемы телефонного мошенничества**

**Звонок из МВД**

Злоумышленник представляется следователем или другим сотрудником госструктур и говорит, что на имя абонента пытались оформить подложный кредит или снять деньги со счёта. Суммы, как правило, называют крупные. В отдельных вариантах сценария фальшивый следователь может суровым тоном задавать разные вопросы, чтобы у жертвы возникло ощущение, что её в чём-то подозревают. Кульминация сценария — перевод звонка на фальшивого сотрудника Центробанка «для уточнения информации». Обескураженная и, возможно, даже напуганная жертва называет данные карты, в том числе CVV-код и срок действия. Зная эти данные, мошенники могут покупать разные товары в интернете от имени владельца карты.

Во-первых, настоящий следователь ничего не может знать о движениях средств по вашему счету. Просто потому что это банковская тайна, и её не предоставляют без решения суда. Во-вторых, реальный следователь просто технически не сможет перевести звонок на сотрудника Центробанка. Свои сомнения можно проверить, позвонив в дежурную часть МВД самостоятельно — так вы уточните реальное наличие сотрудников в ведомстве.

**Помогите бедному менеджеру**

А этот сценарий рассчитан на сочувствие. Мошенник представляется сотрудником банка, где обслуживается жертва, и запинающимся от волнения голосом говорит, что случайно указал его данные при финансовой операции с другим клиентом. Если срочно всё не отменить, его оштрафуют или уволят. А для отмены нужны секретные данные карты. Дальше всё по старой схеме: мошенник узнает CVV-код и обнуляет счёт жертвы.

Сам сценарий далёк от внутрибанковских реалий. Для отмены и коррекции ошибочных операций у сотрудника есть внутренние регламенты — ему не нужно обращаться к клиенту.

**Ваша карта заблокирована**

Классика телефонного мошенничества в новой интерпретации. Жертва слышит в трубке голос банковского робота, который сообщает, что карта заблокирована в связи с подозрительной операцией. Далее робот переводит звонок на псевдосотрудника банка, а дальше как обычно — уточнение информации и сбор секретных данных. Схема работает, потому что у многих жертв голосовые помощники ещё не ассоциируются с мошенничеством, хотя технически имитировать их работу вовсе не сложно.

Ещё один вариант — мошенники не звонят, а присылают SMS-уведомление о блокировке счёта. В нём указывается «безопасный счёт», на который рекомендуется перевести деньги в течение 24 часов. В противном случае банк заблокирует их на долгий срок.

Банковские роботы всегда звонят с коротких номеров, а не обычных абонентских. И главное — для идентификации клиента не нужны секретные данные, такие как CVV-код и срок действия карты. Что касается «безопасных счетов», то у банков вообще нет такого инструмента для клиентов. При блокировке карты дистанционный доступ к ней просто замораживается до выяснения обстоятельств.

**Вас обманули по телефону? Мы поможем!**

Свежий и довольно циничный сценарий, направленный на жертву уже состоявшегося телефонного развода. Мошенник представляется сотрудником юридической компании и сообщает, что потерянные деньги можно вернуть, да ещё и получить с обидчика компенсацию за моральный ущерб. Но для этого нужно оплатить услуги компании (как правило, сумма небольшая по сравнению с предыдущим «уловом» мошенников) или заплатить налог — тут возможны варианты. Обнадёженная жертва переводит деньги на указанный счёт.

Честные юридические компании работают официально, с договорами и чеками. А главное, откуда они узнают про обман?

**Звонок от оператора связи**

Относительно новая схема обмана работает так: мошенники звонят под видом оператора мобильной связи и требуют подтвердить личность. Проще говоря, им нужны паспортные данные. В противном случае «оператор» грозится отключить связь, что, в свою очередь грозит потерей доступа к аккаунтам и банковским картам и счетам, которые привязаны к номеру телефона. На самом деле, полученная личная информация жертвы может быть затем использована для получения кредитов или с другими нечестными целями.

Совет стандартный: не сообщать персональные данные неизвестным лицам. Все вопросы с оператором лучше решать, перезвонив ему самостоятельно.

**Как не попасться на уловки мошенников**

«Это же явный обман!», «Ну как на такое можно повестись?» — подумают многие. Но не стоит забывать, что главные козыри — эффект неожиданности и напор, с которым мошенники общаются с жертвами. Они не дают времени осмыслить и проверить информацию и торопят с принятием решения — такова тактика всех сценариев обмана.

Запомните три правила общения с подозрительными абонентами, и мошенники вас не проведут:

* Не сообщайте CVV и коды, которые приходят в SMS. Настоящие банки никогда не запрашивают эту информацию.
* При малейших сомнениях кладите трубку. Всегда можно уточнить информацию по официальным номерам банков или государственных структур.
* Если абонент вас торопит, агрессирует или давит на жалость, тоже кладите трубку. Представители официальных организаций не должны так общаться.

МТС