

«Дошутились... до списания денег»: почему игры с мошенниками плохая идея

«Да я просто решил с ними поиграть», «Хотел проверить, на что они способны», «Я же понимаю, что это мошенники» — с этих фраз начинается множество историй, которые заканчиваются одинаково: списанными деньгами, заблокированными счетами и недоуменным вопросом: «Ну как так вообще получилось?»

Когда человеку звонят или пишут мошенники, реакция часто уходит в две крайности — панику или самоуверенность. С паникой все понятно. А вот самоуверенность кажется безобидной, особенно когда есть ощущение полного контроля. Но именно в этот момент контроль начинает незаметно ускользать.

Почему «просто поговорить» уже ошибка

Мошенники редко пытаются взломать банк или систему безопасности. Их настоящая цель — человек. Каждый разговор, даже насмешливый или «да я просто прикалываюсь», работает как бесплатный тест.

Пара фраз позволяет преступникам понять, как вы реагируете на давление, насколько быстро принимаете решения, пугают ли вас слова «банк», «полиция», «долг», «кредит», готовы ли вы продолжать диалог и насколько легко вас вывести на эмоции. Им важно не содержание ответа, а сам факт: вы отвечаете, не бросаете трубку. Для мошенника это сигнал: контакт с человеком установлен. Значит, с этим номером можно работать, значит, сюда стоит вернуться.

Первый звонок редко является атакой. Чаще это разведка. Сегодня вы «просто пошутили», завтра этот же голос используют в новой схеме — например, для звонка вашим родственникам. Или разговор станет первым шагом к более точной атаке с правильными словами и подходящим моментом. Послезавтра звонок уже будет «по-настоящему» — от имени банка, службы безопасности или знакомого. Каждый следующий шаг будет выглядеть логичнее и убедительнее предыдущего, потому что сценарий уже подстроен под вас.

«Я ничего не сказал» — распространенное заблуждение

Очень часто пострадавшие говорят: «Я же не называл данные карты», «Я ничего не подтверждал», «Я просто разговаривал».

Но мошенничество давно перестало строиться только на реквизитах и кодах из СМС. Сегодня этого может быть и не нужно. Иногда достаточно подтвердить, что номер активен и на него отвечают, показать, что человек пользуется онлайн-банкингом и понимает, о чем идет речь, понять, что он один и рядом никого нет, кто мог бы подсказать или остановить, услышать голос, интонации и манеру речи — для будущей имитации.

По отдельности это кажется мелочью, но именно из таких деталей складывается психологический пазл. И шутка, «просто разговор», попытка поиграть с мошенником часто становятся его первым кусочком.

Маленькие суммы — большая ловушка

300 тенге за «доставку», 1 000 тенге «для проверки» - списание небольших сумм почти всегда являются тестом для мошенников. Важно не сколько человек потерял, а заметил ли он списание, стал ли разбираться и звонить в банк или решил, что «из-за мелочи» не стоит тратить время.

Если человек молчит и ничего не предпринимает, это сигнал: можно продолжать. После «мелочи» почти всегда следуют повторные списания, скрытые подписки, «возвраты», которые на самом деле новые переводы, попытки оформить кредит.

Есть и психологический момент, человеку стыдно признавать, что его обманули «из-за копеек». Именно это молчание позволяет мошенникам действовать дальше.

Пока человек молчит, банк не знает о схеме и не может вовремя отреагировать, близкие не предупреждены и могут столкнуться с тем же сценарием, а мошенники продолжают использовать уже отработанную схему снова и снова.

Реальные истории, которые начинаются «с шутки»

Мужчине позвонили якобы из банка. Он понял, что звонят мошенники, и решил пошутить, отвечал им, где-то соглашался. Через пару дней пришло сообщение о «бонусе», и он потерял доступ к приложению.

Девушка получила сообщение от «курьерской службы». Решила ради интереса посмотреть, что там. Ввела номер телефона, потом код — «*чтобы проверить*». Денег сразу не списали. Зато ночью с карты ушли все накопления.

Подросток переписывался с мошенником в мессенджере «*ради смеха*». Через неделю с его аккаунта начали писать родственникам с просьбами перевести деньги. Объяснять пришлось долго — и неприятно.

Общее у этих историй одно: на каждом этапе человеку казалось, что он контролирует ситуацию, но это иллюзия.

Что действительно работает?

При любом подозрительном звонке или сообщении важно сразу завершать разговор, самостоятельно перезванивать в банк по официальному номеру, блокировать карту при малейших сомнениях и внимательно проверять операции и уведомления. Не менее важно обсуждать подобные случаи с близкими — особенно с детьми и пожилыми родственниками.

Рекомендации:

1. **Не играйте с мошенниками.** Любая шутка или «проверка» — это сигнал для преступников.
2. **Не переходите по подозрительным ссылкам** и не вводите коды из СМС, даже «для проверки».
3. **Обращайте внимание на мелкие списания.** Даже небольшая сумма может стать первым шагом к серьезным потерям.
4. **Говорите о проблеме вовремя.** Чем раньше вы сообщите в банк или близким, тем меньше шансов у мошенников действовать дальше.
5. **Обсуждайте сценарии с семьей.** Дети, пожилые родственники и друзья должны понимать типовые схемы мошенников.
6. **Не думайте, что вы умнее схемы.** Самоуверенность делает вас уязвимым.

Помните, что мошенники зарабатывают не только на наивности граждан, но и на самоуверенности. Шутка, ирония, «*я все контролирую*» - не защита. Если с вами связались мошенники, вы уже не участник игры. Единственный выигрышный ход — выйти из нее сразу. Там, где кажется, что вы просто разговариваете, на самом деле вас уже внимательно изучают.

Берегите себя, своих близких и повышайте финансовую грамотность.

Материал подготовлен при помощи www.fingramota.kz