



КАК ЗАЩИТИТЬ СЕБЯ ОТ МОШЕННИКОВ?

В среднем в квартал сумма ущерба от действий мошенников приближается к 3 млрд рублей. И по предварительным оценкам, совокупный размер подобных краж за 2021 год не меньше, чем в 2020 году.

Основными каналами действий мошенников по-прежнему остаются телефон и интернет. Злоумышленники пытаются войти в доверие и усыпить бдительность граждан, представляются сотрудниками правоохранительных органов, Банка России или коммерческих банков, в том числе с использованием подменных номеров. Так, мошенники могут предлагать перевести деньги на «безопасный», «специальный» или «защищенный» счет в Центральном банке.

Адам Хазизович Мугу



заведующий сектором платежных систем и расчетов
Отделения-Национального банка
Республика Адыгея

В действительности такого счета нет, а Банк России не работает с физическими лицами как с клиентами, не ведет их счета и по своей инициативе людям не звонит.

ПРИЗНАКИ ОБМАНА:

Первый признак: вам звонят неизвестные, и тема разговора сводится к деньгам. Немедленно прервите разговор, кем бы ни представлялся собеседник. Сотрудники правоохранительных органов, банков, госорганов никогда не требуют по телефону предоставления персональных данных и банковских реквизитов, информацию о счетах и картах. Они не просят перевести деньги якобы на "защищенный счет" или куда-либо еще.

Второй признак: вас просят заплатить налог или штраф по неким реквизитам, внести залог или аванс за товар. Реквизиты для перевода средств как правило принадлежат мошенникам, а после внесения предоплаты за товар «продавец» исчезает.



Третий признак : супервыгодное предложение. Вам предлагают щедрые выплаты, призы, условия по кредитам и депозитам выше рыночного уровня, инвестиционные продукты, обещающие высокую доходность. При этом вас пытаются убедить, что нельзя упускать шанс получить сразу много денег. Либо наоборот – пытаются запугать возможной потерей денег.

Четвертый признак: на вас давят, требуют принять решение немедленно. Мошенники всегда требуют от человека быстрого принятия решений, действуют уверенно и агрессивно. Если чувствуете, что на вас давят, угрожают, заставляют сделать покупку, совершить транзакцию «либо сейчас, либо никогда» – прерывайте общение. Это точно мошенники.

Пятый признак: если запрашивают информацию о банковской карте. Важно помнить, что настоящий сотрудник банка никогда и ни при каких обстоятельствах не будет запрашивать у человека ПИН-код и срок действия карты, трехзначный номер на ее обороте.

Банки обязаны отслеживать подозрительные операции со счетами своих клиентов. Если у банка возникает подозрение, что совершается несанкционированная операция, его представитель может связаться с владельцем счета и уточнить, действительно ли он совершает эту операцию. Владелец счета должен только подтвердить или не подтвердить операцию – на этом общение заканчивается.

ОБЩИЕ ПРАВИЛА

- Нельзя сообщать незнакомым людям данные своей банковской карты (номер карты, срок действия, трехзначный код на ее обратной стороне), а также ПИН-код.
- При оплате банковской картой в торговой или сервисной точке не теряйте карту из виду и прикрывайте клавиатуру рукой, набирая ПИН-код.
- Не вводите данные банковской карты на непроверенных сайтах, а требование ввести ПИН-код в сети Интернет вообще незаконно.
- Если звонок из банка вызвал сомнения, ни в коем случае не перезванивайте в ответ. Необходимо положить трубку, набрать телефон вашего банка (он есть на карте или на официальном сайте) только в КНОПОЧНОМ (РУЧНОМ) режиме, не используя автодозвон.
- Используйте отдельную карту для онлайн-платежей и кладите на нее нужную сумму непосредственно перед покупкой.
- Не используйте одинаковые пароли для входа в свои аккаунты на разных сайтах и не публикуйте в соцсетях конфиденциальную информацию о себе.

- Не переходите по ссылкам в письмах от незнакомых пользователей.
- Установите на все свои устройства с выходом в интернет антивирус и регулярно обновляйте его.
- Не публикуйте в открытом доступе в соцсетях свои персональные данные: номер мобильного телефона, адрес, данные паспорта. Вся эта информация может быть использована мошенниками.

ЕСЛИ ВЫ СТАЛИ ЖЕРТВОЙ МОШЕННИКОВ, необходимо:

- Немедленно обратиться в свой банк и сообщить о хищении.
- Заблокировать карту.
- Написать заявление о несогласии с операцией.
- Обратиться с заявлением в полицию.