**Закрыть счета: мошенники освоили еще один метод.**

Мошенники придумали новую схему обмана доверчивых держателей банковских карт. Злоумышленники, как и раньше, звонят жертве по телефону, но уже подбирают иные слова. Теперь они предлагают клиенту закрыть счет в банке. Как только тот отказывается от услуги, то тут же попадается на крючок преступников.

Преступники сгенерировали очередной вариант кражи средств с банковских карт россиян. Об этом сообщает газета «Известия» со ссылкой на директора Банковского института ВШЭ Василия Солодкова.

По словам специалиста, сотрудники нелегальных call-центров начали использовать измененный сценарий общения, который пока вызывает больше доверия, чем предыдущие телефонные аферы. Если раньше мошенники «маскировались» под службу безопасности банка и сообщали потенциальной жертве о блокировке счета в связи с подозрительной транзакцией, то теперь злоумышленники задают вопросы о том, в каком отделении и когда клиент хочет закрыть счет. При этом они для большей убедительности говорят жертве, что банк уже получил заявление от нее с просьбой закрыть счет в финансовой организации.

Когда же держатель банковской карты указывает, что не просил о данной услуге, то запускается ключевой механизм аферы. Мошенники тут же предлагают перевести деньги на якобы безопасный счет, утверждая, что клиент стал жертвой хакеров и может в любую минуту лишиться своих сбережений. Но для того, чтобы спасти деньги, сотруднику банка нужна личная информация о счете клиента. Мошенник просит назвать реквизиты карты, ССV-код на ее обратной стороне и срок действия «пластика». Как только жертва называет эти данные, преступники тут же переводят деньги уже на свой счет. Доказать потом неправомерность подобной транзакции будет сложно, а вернуть деньги почти невозможно, предупреждают эксперты.

Выявлением нового способа краж уже занимаются сотрудники Банка России. Несмотря на то что мошенники предлагают прийти лично в банк, их способ кражи не предусматривает физических контактов. По его словам, схема сводится к тому, чтобы перевести средства на счет преступников. Впрочем, возможным это станет, только если клиент сообщит свои персональные данные для перевода денег на «безопасный счет».

Несмотря на простоту и прозрачность схемы, россияне все чаще стали попадаться на подобные уловки мошенников. В конце прошлого года сообщалось, что за последние несколько лет наиболее популярным способом кражи денег с банковских счетов россиян стали телефонные звонки.

Если еще в 2017 году об этой проблеме рассказали 160 тысяч раз, а в 2019 году количество жалоб возросло до почти 2,5 млн.

По данным МВД России, в период с января по сентябрь прошлого года мошенники провернули около 103 тыс. хищений с банковских карт. По сравнению с аналогичным периодом 2018 года показатель увеличился более чем в четыре раза.

По мнению опрошенных «Газетой.Ru» экспертов, такой вид кражи связан с ликвидацией технических уязвимостей систем, а также дешевизной способа.

Особенно в последнее время набирают популярность схема, при которой деньги с карты похищают, заменив номер телефона, к которому «привязана» карта в банке. В течение последних двух лет растет количество хищений средств с карт клиентов с помощью методов социальной инженерии, когда человека при звонке на мобильный телефон сначала запугивают тем, что с его карты списывают средства неизвестные люди, а затем принуждают выдать коды и пароли от карты.

Злоумышленники вновь применяют максимально простую схему: на мобильный телефон поступают звонки и смс-сообщения с просьбой перезвонить. В качестве отправителей указывают Центробанк, CentroBank, Службу безопасности Банка России, Visa, MasterCard, «МИР» или службу банка, в котором обслуживается клиент.

Если клиент перезванивает по указанному телефону и сообщает свои данные, мошенники могут снять деньги с карты, изготовив ее дубликат или заменив при обращении в банк номер телефона владельца карты. Затем злоумышленники переводят деньги с карты жертвы на свои счета или рассчитываются за покупки в интернете, подтвердив операции с помощью кода, полученного в смс.

Для потерпевшего ситуация осложняется тем, что исчезновение денег он часто обнаруживает только через несколько дней после происшествия. Дело в том, что смс о списании средств приходят уже не на его номер телефона, а на номер мошенников.

Примечательно, что даже если держатель карты сумел уйти от телефонных мошенников, то деньги у него с карты все равно могут похитить, причем прямо у банкомата в отделении банка. В прошлом году преступники придумали новый способ запугивания клиентов.

Злоумышленники якобы забывают карту в банкомате, а затем ждут, пока ее вытащит следующий человек в очереди. Как только жертва дотронулась карты, то тут же появляется «забывчивый» клиент.

Он проверяет баланс, обнаруживает якобы пропажу средств и начинает обвинять в краже вернувшего ему карту клиента.Обычно речь идет о сумме от 5 до 15 тысяч рублей.

В этот момент появляется свидетель, который подтверждает версию «пострадавшего» и советует тому вызвать полицию. Злоумышленник соглашается и начинает запугивать жертву, утверждая, что на карте остались отпечатки его пальцев. В итоге пострадавший клиент под прессингом двух мошенников в большинстве случаев сдается и уже сам соглашается вернуть якобы украденные деньги.

<https://www.gazeta.ru/business/2020/02/10/12952741.shtml?utm_source=yxnews&utm_medium=desktop&utm_referrer=https%3A%2F%2Fyandex.ru%2Fnews>