Waybank

Главные признаки телефонного мошенничества

Мошеннических схем много, и регулярно появляются новые. Чтобы не стать жертвой обмана, полезнее знать не столько сами схемы, сколько ключевые признаки того, что вы столкнулись с мошенником. Тогда меньше шансов остаться без денег.

По статистике в четырех из пяти случаев мошенничества клиенты банков теряют свои деньги не из-за хакерской атаки, а из-за того, что сами их отдают или сообщают мошенникам реквизиты карт. Обычно мошенники выуживают номер и срок действия карты, трехзначный CVV/CVC-код, а также пароли и коды из СМС, которые банки присылают для подтверждения операций. То есть киберпреступники - это по большей части не столько хакеры, сколько психологи, которые «взламывают» не компьютер (ноутбук, телефон, планшет и другое), а сознание своей жертвы.

По каким же признакам можно распознать мошенников?

1) На вас выходят сами

Кто-то сам вам звонит (пишет письмо, присылает ссылку и так далее). Вне зависимости от того, кем он представляется, - сотрудником банка, полиции, магазина, братом миллионера из Нигерии - и чего он хочет, надо быть осторожным. Помните: если кто-то незнакомый звонит вам, значит ему что-то нужно. Вопрос: что?

В настоящее время Банком России фиксируется увеличение количества случаев телефонного мошенничества с использованием следующего сценария:

Злоумышленники звонят клиентам кредитных организаций и представляются сотрудниками правоохранительных органов Российской Федерации, после чего сообщают о наличии в производстве материалов уголовного дела, открытого в отношении потенциальной жертвы по заявлению Банка России.

Используя этот предлог, злоумышленники, побуждают клиентов кредитных организаций предоставить им сведения, относящиеся к персональным данным и к информации, составляющей банковскую тайну, в том числе информацию о последних операциях, проведенных жертвой по открытым банковским счетам. В дальнейшем данная информация используется злоумышленниками при дистанционной верификации с использованием телефонной связи (зачастую указанная информация запрашивается финансовыми организациями при верификации клиентов с использованием телефонной связи).

2) Разговор касается денег или вашей банковской карты

Важно помнить, что у мошенников единственная цель - ваши деньги. Ключ к ним - банковская карта. Жулики либо вынуждают человека самого отдать деньги, либо выуживают у него информацию (например, данные карты), которая позволит эти деньги украсть. Если вас просят перевести деньги на некий счет, заплатить налог, бронь, штраф, внести залог, аванс или совершить другие действия, связанные с денежным переводом или раскрытием данных карты, - это скорее всего мошенники.

3) Делают супер-выгодное предложение или пугают

Вам делают супер-выгодное предложение: щедрые выплаты, призы, невероятно привлекательные условия по кредитам и депозитам, инвестиционные продукты, обещающие огромную доходность. При этом вас убеждают, что нельзя упускать шанс

получить сразу много денег, надо обязательно использовать уникальную возможность. Противоположная схема - вас пытаются запугать: деньги вот-вот украдут, спишут со счета, вы лишитесь потенциального дохода.

Имейте в виду, что у мошенников всегда заготовлены ответы на возможные вопросы. Поэтому даже не пытайтесь вступать с ними в беседу, ведь чем дольше вы беседуете, тем крепче вас «подсаживают на крючок».

Помните, если вам обещают многое, требуя взамен малое, то вы лишитесь либо малого, либо всего, что есть на карте, но так и не получите ничего взамен.

4) Морально давят, требуют принять решение немедленно

Мошенники работают с большим количеством людей. Им некогда долго возиться с каждым в отдельности. Кроме того, их задача - не дать жертве опомниться. Поэтому они всегда требуют от человека быстрого принятия решений, действуют уверенно и агрессивно. Если вы чувствуете, что на вас давят, угрожают, ставят условие сделать покупку, совершить транзакцию «либо сейчас, либо никогда» - прерывайте общение. Это точно мошенники.

5) Запрашивают информацию о банковской карте

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. Мошенники же начинают выуживать разные данные: коды из СМС, номер карты, трехзначный код на ее обратной стороне, ПИН-код и так далее. Важно помнить, что настоящий сотрудник банка никогда и ни при каких обстоятельствах не будет запрашивать у человека данные его карты. Если кто-то пытается это сделать, прервите разговор - вы общаетесь с мошенником.

Если вы будете всегда помнить об этих признаках, то вне зависимости от хитрости и новизны мошеннической схемы, не попадете в расставленные сети. Важно понимать, что каждый из этих признаков в отдельности не является однозначным доказательством того, что с вами говорят мошенники (кроме случаев, когда у вас запрашивают трехзначный код на обратной стороне банковской карты, ПИН-код или код из СМС). Но чем больше таких признаков, тем больше вероятность того, что вас пытаются обмануть.

Если после разговора с незнакомцем у вас возникли какие-то сомнения или вопросы, перезвоните в свой банк по номеру телефона, указанному на его сайте или банковской карте, и уточните интересующую вас информацию.

О все случаях подозрительных звонков, с попыткой получить информацию по клиенту Банка, просим сообщать в Банк.