Как не стать жертвой мошенников

Аферисты постоянно придумывают новые схемы обмана. Как правило, эксплуатируют актуальную информационную повестку: в 2020 году это была пандемия коронавируса, в начале 2022 года на пике популярности была тема санкций, а сейчас, скорее всего, появятся новые сценарии в связи с мобилизацией. Единственный способ избежать денежных потерь — критически воспринимать любые предложения, перепроверять информацию и никогда не торопиться при принятии финансовых решений.

Верные признаки, по которым можно вычислить мошенников:

1. На вас выходят сами

Вам звонит незнакомец, присылает СМС-сообщение, электронное письмо или ссылку в мессенджере. Кем бы он ни представился — сотрудником банка, полиции, магазина — насторожитесь. Раз он стал инициатором контакта, ему что-то от вас нужно. Быстро проверить, тот ли он, за кого себя выдает, не получится. Номер, который высвечивается при входящем вызове, можно подменить, аккаунты или сайты известных людей или организаций – подделать. Так что стоит быть бдительным и никому не верить на слово.

2. С вами говорят о деньгах

Основная задача мошенников — получить доступ к чужим деньгам. Схемы обмана почти всегда связаны с финансами: вам предлагают перевести все деньги на «безопасный счет», оплатить «страховку для получения кредита» или «очень выгодно» инвестировать свои сбережения.

3. Вас просят сообщить персональные данные

Если ворам нужны ключи от квартиры, то мошенникам — ключ к деньгам на ваших счетах. Это конфиденциальные данные вашей карты: номер, срок действия и три цифры с ее обратной стороны; логины и пароли к личному кабинету на сайте банка или мобильному приложению; СМС и push-коды из банковских уведомлений. Знайте, что настоящий сотрудник банка никогда не спросит секретные реквизиты карты, ПИН-коды и пароли! Если банк замечает сомнительный платеж или перевод с вашего счета, с вами связываются только чтобы подтвердить или отклонить операцию. Конфиденциальные данные для этого не требуются. Если о них спрашивают — будьте уверены, звонят не из банка и вас точно пытаются обмануть.

4. Вас выводят из равновесия

Мошенники стремятся вызвать сильные эмоции – напугать или обрадовать. Так они сбивают с толку и притупляют бдительность потенциальной жертвы. Например, сообщают: «Ваш онлайн-банк взломали!», чтобы вы от растерянности выполнили любые просьбы и выдали любую информацию, лишь бы спасти деньги. Либо, наоборот, огорошивают новостью о внезапном выигрыше в лотерею или обещают быстрое обогащение. Взамен вы должны будете «лишь оплатить небольшой взнос», а для этого — ввести данные банковской карты на сайте. Мошенники создают фишинговые (фальшивые) страницы, с помощью которых

воруют данные карт и получают доступ к счетам доверчивых пользователей. Всегда сохраняйте здоровый скептицизм и не торопитесь следовать чужим инструкциям, как бы ни были взволнованы.

5. На вас давят и торопят

Мошенники всегда торопят, чтобы не дать вам времени обдумать ситуацию. Вас принуждают к чему-то, ставят условия: «сейчас или будет поздно». Ситуация, в которой вам не дают права выбора и заставляют немедленно действовать, подозрительна. Если чувствуете психологический дискомфорт, лучше сразу же прекращайте общение. Ведь чем дольше вы разговариваете с мошенником, тем сильнее он будет на вас давить. На все ваши расспросы у обманщиков есть заготовленные ответы, которые только нагнетают обстановку.

Следуйте базовым правилам финансовой безопасности:

· Лучше всего вообще не отвечать на звонки с незнакомых номеров (как мобильных, так и стационарных), особенно если вы не ждете звонка.

· Если ответили, и незнакомец завел разговор, который так или иначе касается денег, сразу прервите беседу: чем дольше вы общаетесь со злоумышленником, тем у него больше шансов «заболтать» вас и развести на деньги.

· Если звонивший незнакомец сообщил что-то типа «сохранность ваших средств банковском счете под угрозой», «на вас пытаются оформит кредит» и т.п., вы прервали разговор, но сомнения остались, позвоните в ваш банк, но ни в коем случае не ответным звонком на номер, с которого поступил звонок! Это тоже может быть частью преступной схемы. Надо набрать номер самостоятельно: телефон банка есть на вашей карте или найдите его в интернете на официально сайте.

· Никому ни при каких обстоятельствах не сообщайте полные реквизиты банковской карты, включая трехзначный код с обратной стороны; а также ПИН-коды и пароли из СМС от банка.

· Не переходите по сомнительным ссылкам из сообщений.

· Не переводите деньги, не оформляйте кредит под диктовку звонящего. Настоящие сотрудники банка или других официальных структур никогда не просят делать это по телефону.

· Не храните много денег на карте, которой расплачиваетесь в интернете: кладите только ту сумму, которую собираетесь потратить в данный момент. В этом случае, даже если мошенники попытаются украсть деньги, им не удастся вывести слишком много.

· Не соглашайтесь сходу ни на какие заманчивые предложения — будь то «выгодный кредит» или внезапная компенсация. Дайте себе время на размышление, посоветуйтесь со знакомыми, проверьте информацию о компании и «уникальной акции», которую она вам рекламирует.

· Не публикуйте в открытом доступе – например, в соцсетях - свои персональные данные: номер телефона, домашний адрес, данные паспорта. Мошенники охотно задействуют эту информацию в своих аферах.

· Помните, Банк России, он же Центробанк, никогда не звонит и не рассылает сообщения гражданам.

· Установите антивирус на все устройства и обновляйте его.

По статистике в большинстве случаев люди теряют свои сбережения не потому, что их счета взламывают хакеры. Владельцы банковских карт чаще всего сами сообщают мошенникам конфиденциальные сведения: реквизиты карты, включая номер, срок действия, трехзначный CVV/CVC-код, а также пароли и коды из СМС, которые банки присылают для подтверждения операций.

А как быть тем, кто стал жертвой мошенников?

· Если телефонные мошенники похитили ваши деньги, немедленно заблокируйте карту. Это можно сделать в мобильном приложении или личном кабинете на сайте банка, а также через контакт-центр банка (телефон указан на оборотной стороне карты) или в любом его отделении.

· Как можно быстрее, максимум в течение суток после списания средств напишите заявление в отделении банка о несогласии с операцией и обратитесь с заявлением о хищении денег в любое отделение полиции.

· Во всех случаях мошенничества или подозрения на мошенничество, обращайтесь в Банк России – через интернет-приемную на сайте либо по номеру горячей линии: 8-800-300-30-00 и 300 для звонка с мобильных. Звонок бесплатный.