

КАК БЫСТРО РАСПОЗНАТЬ МОШЕННИКА

У Ивана Сергеевича зазвонил телефон, номер был незнаком. Солидный мужской голос на фоне шума офиса звучал встревоженно: «Добрый день. Иван Сергеевич? Это служба безопасности банка «Лапша-Финанс». Мы зафиксировали, что киберпреступники пытаются получить доступ к вашему личному кабинету. Надо срочно перевести все деньги на безопасный счет, иначе их украдут!» Иван Сергеевич немедленно положил трубку. Рассказываем, по каким признакам он вычислил обманщиков.



Аферисты постоянно придумывают новые способы выманить у людей деньги или конфиденциальные данные для доступа к счетам. Но какой бы ни была легенда, есть пять примет, по которым можно сразу же вычислить мошенников.

Признак 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, вашим троюродным братом-миллионером из Зимбабве — 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.

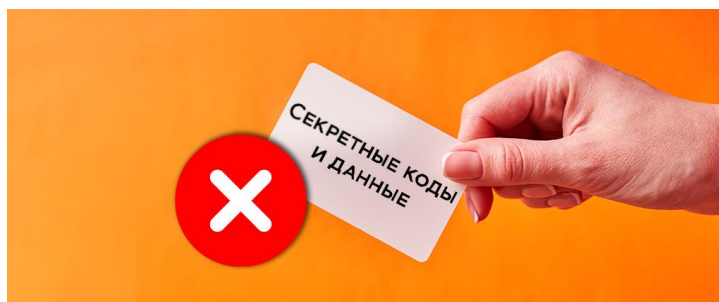
Признак 2. С вами говорят о деньгах.

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 (на самом деле — в финансовую пирамиду).

«На днях бабушке позвонили якобы из службы безопасности ее банка. Сказали, что с ее карточки кто-то только что попытался украсть деньги.»

Они операцию заблокировали, но деньги надо срочно перевести на некий безопасный счет...»

Легенды могут быть какими угодно, но речь всегда про деньги — которые вы можете потерять или получить.



Признак 3. Вас просят сообщить данные.

Если вору нужны ключи от квартиры, то социальным инженерам— «ключ» к деньгам на ваших счетах. Это могут быть конфиденциальные данные вашей карты, включая срок действия и три цифры с ее обратной стороны. Либо логины и пароли к личному кабинету на сайте банка или мобильному приложению. И почти всегда — коды из банковских уведомлений.

Настоящий сотрудник банка никогда не спросит секретные реквизиты карты, ПИН-коды и пароли.

Когда банк замечает сомнительный платеж или перевод с вашего счета, с вами связываются, чтобы подтвердить или отклонить операцию, и только. Конфиденциальные данные для этого не требуются. Если о них спрашивают — будьте уверены, звонят не из банка и вас точно пытаются обмануть.

Признак 4. Вас выводят из равновесия.

Мошенники стремятся вызвать у вас 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 и волнения 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 страницы, с помощью которых воруют данные карт и получают доступ к банковским счетам доверчивых пользователей.

«Участвовала в конкурсе в соцсети Instagram около месяца назад, где призом была любая вещь, которую я выберу, размещенная на странице. Я выбрала кроссовки, написала организаторам, после чего мне предложили оплатить доставку в размере 450 Р...»

Всегда сохраняйте здоровый скептицизм и не торопитесь следовать чужим инструкциям, как бы ни были взволнованы.



Признак 5. На вас давят.

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.

«Попал в ужасную ситуацию. Позвонили из моего банка, назвали мое ФИО и попросили подтвердить, что я сейчас оформляю кредит на 550 000 рублей. Я очень удивился, потому что ничего не оформлял в тот момент. Сотрудник банка сказал, что если это не я, значит мошенники пытаются взять кредит от моего имени, поэтому надо срочно принять меры».

Никогда не принимайте поспешных решений, особенно если они касаются ваших финансов. Всегда берите паузу, чтобы разобраться в том, что происходит. Возьмите за правило перепроверять любую информацию в первоисточнике.

Звонят из банка с тревожными новостями? Положите трубку и наберите номер горячей линии банка сами, чтобы прояснить реальное положение дел.

Прислали странное уведомление от имени Федеральной налоговой службы (ФНС)? Заведите личный кабинет на сайте ФНС — в нем можно проверить суммы налогов и сразу же оплатить их.

Получили «письмо счастья» о государственной выплате? Поищите новости об этом в деловых СМИ. А еще лучше — найдите сам закон, указ или постановление, которые вводят выплаты. Обратите внимание на условия, кому они положены.

Не всегда при общении с аферистом вы заметите все пять признаков мошенничества. Но в любой ситуации стоит проявить бдительность.