Киберпреступники все чаще маскируют свой номер под официальные номера банков. Разбираемся, как не попасться на уловки мошенников.

Для начала проверьте, точно ли это сотрудник банка. Положите трубку, позвоните по официальному номеру банка и уточните, все ли в порядке с вашими счетом и картой.

Почему стоит положить трубку и набрать официальный номер банка самому?

Даже если у вас на телефоне высветился знакомый номер банка, ни в коем случае не делайте на него обратный звонок. Наберите номер горячей линии банка вручную. Телефон горячей линии можно найти на обратной стороне банковской карты или на официальном сайте банка.

Такая бдительность может показаться параноидальной. Но в последнее время киберпреступники все чаще подделывают официальные телефонные номера банков, чтобы обмануть их клиентов.

Мошенники используют специальное программное обеспечение, которое помогает скрыть настоящий номер звонящего, при этом на телефоне человека отражается официальный номер банка. Обычно преступник обращается к собеседнику по имени и отчеству, может назвать фамилию и даже номер и срок действия карты. Эти сведения мошенники, как правило, получают заранее из открытых источников, например из социальных сетей, и с помощью фишинга.

Даже если информация звучит очень правдоподобно, лучше перестраховаться и позвонить в банк самому, чтобы общаться точно с его сотрудником, а не с преступником.

Чаще всего обманщики звонят поздно вечером, ночью или ранним утром в выходные дни, когда человек спит и не может быстро сориентироваться. Преступник представляется

сотрудником банка и сообщает о подозрительной операции, которая требует немедленных действий со стороны клиента. Мошенники хорошо знакомы с психологией: говорят быстро и уверенно, используют профессиональные термины, нередко фоном включают звуки, имитирующие работу оживленного колл-центра. Все это помогает им втереться в доверие к клиенту банка и сделать так, что он потеряет бдительность.

При этом они торопят и запугивают клиента, давят на его эмоции и уверяют, что случится что-то непоправимое.

Например, обманщики говорят, что по карте проводится подозрительный платеж на крупную сумму и чтобы его остановить, нужно срочно сообщить данные карты, ПИН-код или одноразовый пароль из СМС-сообщения. Если человек колеблется или отказывается их назвать, ему угрожают, что деньги с его карты прямо сейчас уйдут к мошенникам.

Если преступникам удается узнать нужную им информацию, они получают доступ к счету и снимают с него все деньги.

Как защитить свои деньги от мошенников?

Если клиент сам сообщит преступникам секретную информацию, которую нельзя разглашать, вернуть деньги через банк не получится. Поэтому стоит придерживаться основных правил безопасности, чтобы не поддаться на уловки мошенников и не потерять деньги:

1. Всегда набирайте только официальный номер банка. Он указан на обратной стороне карты и на официальном сайте банка.

2. Не перезванивайте и не отправляйте СМС на незнакомые номера, не спешите переходить по ссылкам из сообщений «от банка». В любой непонятной ситуации звоните в банк по официальному номеру и уточняйте информацию у оператора.

3. Если вам звонят из банка, финансовой организации или госоргана, уточните ФИО и должность звонящего и скажите, что перезвоните ему сами. Положите трубку и перезвоните по официальному телефону организации или на горячую линию банка. Номер нужно набрать вручную.

4. Не стоит паниковать и спешить. Если банк выявит подозрительную транзакцию, он сразу приостановит ее на срок до двух суток. За это время вы можете либо подтвердить эту операцию банку, либо отменить ее. Это решение надо принять в течение 48 часов – этого времени достаточно, чтобы хорошо все обдумать и без спешки самостоятельно позвонить в банк. Если же вы ничего не сделаете, то через двое суток банк автоматически снимет блокировку и операция пройдет.

5. Ни под каким предлогом никому не сообщайте личные данные, реквизиты карты и секретную информацию: CVC/CVV-код на обратной стороне карты, коды из СМС и ПИН-коды. Называть кодовое слово можно, только если вы сами звоните на горячую линию банка.