**Как определять звонки злоумышленников**

Банки нечасто сами звонят своим клиентам. Преобладающее количество звонков и смс от банка носят информационный или рекламный характер: предложение нового продукта, роботизированное информирование. Лишь в редких случаях о подтверждении произведенной операции или блокировке счета. Как понять, что звонит сотрудник банка или смс действительно из банка, а не мошенник в [интервью Банки.ру](https://www.banki.ru/news/daytheme/?id=10995579) рассказала эксперт проекта НИФИ Минфина России «Моифинансы.рф» Мария Соловиченко.

Не всегда легко узнать, кто действительно звонит: мошенник или банк. Негативная практика телефонного мошенничества многих уже приучила вообще не брать трубку с незнакомых номеров, ввиду чего случается, что даже полезные звонки остаются без ответа. Для связи с клиентом финансовые организации чаще всего используют короткие телефонные номера (из 3-5 цифр)-с этих номеров происходит рассылка банковских СМС (о состоянии счета, балансе карты, последних операциях, предложениях по депозитам и кредитованию). Звонки из банка также могут поступать как с коротких номеров, так и с «городских» официальных телефонных номеров банка.

Мошенники также пытаются копировать официальные номера: используют подменные или очень похожие. Самый простой способ узнать, кто звонит или шлет смс-внести телефонный номер банка в контакты своего телефона (например, сохранить короткий номер 900 как «Сбер» или 1000 – «ВТБ»). Тогда при использовании «подмены» сохраненное название контакта отражаться не будет. Вместо этого появится +7-9ОО или +7 1 000 (или другие вариации). Городские номера можно проверить на официальном сайте банка или позвонив в колл-центр (в том числе, из банковского приложения). Если вы действительно ждете звонок из банка (по ипотечной сделке, кредитованию и другим вопросам), заранее узнайте, с какого номера вам будут звонить. Нередко в качестве «защиты» от мошеннических звонов используют программное обеспечение-антиспамы –всегда нужно использовать только официальные источники для скачивания и обращать внимание, какую именно информацию о пользователе собирает эта программа, на доступ к чему запрашивает разрешение.

Если же разговор с незнакомого номера состоялся, важно обращать внимание на следующие моменты:

- сотрудник банка никогда не просит перевести деньги на безопасный счет, не просит коды и пароли, не запрашивает информацию о сумме средств на счете. Для идентификации клиента обычно используется кодовое слово или ответ на контрольный вопрос, просьба назвать первые или последние цифры паспорта/карты или номер дома из адреса регистрации (только часть конфиденциальной информации, а не целиком) Все сообщения носят прежде всего информационный характер. Даже при приостановлении подозрительной операции или блокировке карты настоящий сотрудник банка не просит данные клиента или счета, а лишь сообщает о случившемся и озвучивает алгоритм действий клиента, который нужно совершить без участия звонящего (обратиться в отделение, отправить платеж повторно);

- реальный сотрудник банка ограничен во времени (он должен помочь клиенту, но не старается удержать его на линии принудительно): не «обрабатывает», не запугивает и не тянет время. А вот аферист никуда не спешит, нередко упоминает «законодательство» и «уголовную ответственность». Если происходит давление, а «специалист» грубит, допускает пренебрежение и его речь грешит ошибками – это практически гарантированно мошенник.

Банк не сообщает клиенту о чьей-то попытке похитить средства со счета. Если выявлена подозрительная активность, производится блокировка карты и/или операций по счету. Именно об этом может поступить информация из банка. Клиенту может быть рекомендовано заблокировать и перевыпустить карту. Максимум из банковских данных, которые может запросить сотрудник –это последние 4 цифры банковской карты, но никогда не запрашиваются коды из банковских сообщений, пароли и код безопасности с обратной стороны карты, а также не запрашиваются полные паспортные данные, полный номер карты или счета. Если есть сомнения в правомерности запроса каких-либо данных, нужно прекратить разговор и позвонить в банк самостоятельно (по официальному короткому номеру или на горячую линию), либо связаться с банком через чат мобильного банковского приложения. Если звонок был действительно из банка, он не «потеряется». Если прервать разговор и после связаться с банком самостоятельно, беседа будет продолжена другим специалистом.