Доверяй, но проверяй! Как распознать фальшивый телефонный номер банка?

Фото Волго-Вятского ГУ Банка России

В последнее время мошенники все чаще подделывают официальные телефонные номера банков, чтобы обмануть их клиентов. Для этого они используют специальное программное обеспечение, которое помогает скрыть настоящий номер звонящего. При этом на экране телефона потенциальной жертвы обмана отображается номер, совпадающий с официальным телефонным номером банка, находящимся в свободном доступе в сети Интернет.

Как распознать фальшивый телефонный номер банка и какие меры необходимо предпринять для защиты своих денег от мошенников, рассказывают специалисты Отделения Киров Волго-Вятского ГУ Банка России.

Если вам поступил звонок якобы от «службы технической поддержки» или от «клиентского сервиса» банка, убедитесь, точно ли это сотрудник банка. Спросите его ФИО, название подразделения банка и скажите, что перезвоните позже. После этого позвоните по номеру горячей линии банка, указанному на обратной стороне банковской карты или на его официальном сайте, и попросите соединить с сотрудником, который вам звонил.

Ни в коем случае не перезванивайте на высветившийся у вас на телефоне номер. Даже если собеседник обращается к вам по имени и отчеству, использует профессиональные

термины, называет полные реквизиты карты и ваши паспортные данные. Эти сведения злоумышленники могли получить заранее из открытых источников, например, из социальных сетей и с помощью фишинга.

Точно так же нужно реагировать, если вы получили СМС-сообщение, письмо на электронную почту или любое другое уведомление от имени банка. Никогда не отвечайте на него. Самый безопасный вариант — самому позвонить на горячую линию банка.

Не паникуйте и не спешите переходить по ссылкам, если вам говорят «сработала система безопасности. В этот момент по вашей карте проводится подозрительная операция. Чтобы ее остановить, нужно назвать ПИН-код и одноразовый пароль из СМС-сообщения». Помните, что сотрудники банка не будут звонить клиентам из-за подозрительной операции: банк ее просто приостановит на срок до двух суток. За это время вы можете либо подтвердить эту операцию банку, либо отменить ее. Если же вы ничего не сделаете, то через двое суток банк автоматически снимет блокировку и операция пройдет.

Что также должно насторожить при поступлении звонка или сообщения?

Чаще всего мошенники звонят поздно вечером, ночью или ранним утром в выходные дни, когда вы спите и не может сориентироваться. Весь разговор происходит в быстром темпе, чтобы вы не успели опомниться и засомневаться. Преступники торопят и запугивают вас, давят на ваши эмоции и уверяют, что может случиться непоправимое. При этом постоянно звучат фразы «мы действуем в целях вашей безопасности», «мы как банк обязаны обеспечить вашу безопасность» и прочие обороты со словом «безопасность». Все это должно вас насторожить. Особенно, если «псевдосотрудник» банка просит вас сверить все персональные данные и назвать кодовое слово, ПИН-код или СМС-сообщение.

Чтобы не попасться на уловки мошенникам и не потерять свои деньги, придерживайтесь основных правил безопасности.

- Всегда звоните только на официальный номер банка, указанный на обороте карты или на его сайте.
- Не перезванивайте и не отправляйте СМС-сообщения на незнакомые номера, не спешите переходить по ссылкам из сообщений «от банка».
- Никому не сообщайте ваши персональные данные, реквизиты банковской карты и секретную информацию: CVC/CVV- код на обратной стороне карты, ПИН-код и одноразовые пароли. Секретная информация предназначена только для владельца карты. Даже настоящей сотрудник банка не должен её знать.
- Называйте свое кодовое слово только в том случае, если вы сами звоните на горячую линию банка.
- Будьте бдительны и не публикуйте без особой необходимости свой телефонный номер.

С информацией о других видах мошенничества на финансовом рынке, а также о том, как уберечь себя и близких от злоумышленников и что делать, если вы стали их жертвой, можно ознакомиться на информационно-просветительском ресурсе, созданном Банком России, - Fincult.info.