**Звонок «из банка»: как жителям Чечни не стать жертвой мошенников**

В России активизировались мошенники, которые звонят от имени банков с использованием технологии подмены номера. Представляясь сотрудниками финансовых учреждений, они пытаются выведать у банковских клиентов секретную информацию, которую нельзя передавать третьим лицам. Для защиты своих средств Отделение Банка России по Чеченской Республике рекомендует соблюдать простые правила.

 Для начала стоит удостовериться в том, что на другом конце провода действительно находится банковский работник. Для этого следует уточнить его фамилию, имя, отчество, название подразделения и сказать, что перезвоните позже. Затем следует позвонить по официальному номеру банка и попросить соединить с тем сотрудником, который вам звонил.

«За счет специального программного обеспечения кибермошенникам удается скрыть свой настоящий номер, при этом на экране отображается официальный номер банка. Поэтому делать обратный звонок на номер, который у вас высветился, не нужно. Не поленитесь набрать номер горячей линии банка вручную. Его можно найти на обратной стороне банковской карты или на официальном сайте банка», - прокомментировал Иса Тамаев, управляющий Отделением-Национальным банком по Чеченской Республике Южного главного управления Центрального банка Российской Федерации.

Чтобы усыпить бдительность собеседника, злоумышленник обращается к нему по имени, отчеству, может назвать фамилию и даже номер и срок действия его карты. Представляясь сотрудником банка, кибермошенник сообщает о попытках несанкционированного списания средств. Чтобы приостановить операцию, требует незамедлительных действий со стороны собеседника.

«Будучи тонкими психологами, мошенники используют массу приемов, чтобы заслужить доверие своего собеседника. Для имитации колл-центра они разыгрывают правдоподобные сценарии разговора, включают фоновую музыку, говорят профессиональным языком. При этом злоумышленники торопят и запугивают собеседника. В результате сбитый с толку человек нередко сообщает мошенникам данные карты, CVC или CVV-код (три последние цифры на обороте карты) или одноразовый пароль из СМС-сообщения. Благодаря этим данным кибермошенники получают доступ к счету своей жертвы. В случаях, когда клиент банка сам сообщил аферистам конфиденциальные данные, которые нельзя передавать третьим лицам, вернуть похищенные деньги через банк уже не получится», - рассказал Иса Тамаев.

Чтобы обезопасить свои средства, Отделение Банка России по Чеченской Республике рекомендует не перезванивать и не отправлять СМС на незнакомые номера, не переходить по ссылкам из сообщений «от банка». Если банк выявит подозрительную операцию, он сразу приостановит ее на срок до двух суток. Этого времени достаточно, чтобы клиент мог подтвердить или отменить операцию. Ни в коем случае нельзя никому сообщать личные данные, реквизиты карты и секретную информацию: CVC/CVV-код на обратной стороне карты, коды из СМС и ПИН-код. Называть кодовое слово можно, только если вы сами позвонили на горячую линию банка.