**Жителям Чечни рассказали, как защитить свои средства от телефонных мошенников**

Чем эффективнее банки отражают хакерские атаки, тем изворотливее становятся киберпреступники, которые придумывают все новые способы хищения денег с банковских карт. В числе новых схем мошенничества и маскировка телефонного номера под официальные номера банков. С помощью специального программного обеспечения лжебанкиры скрывают свой настоящий номер, при этом на телефоне отображается официальный номер банка. Представляясь сотрудниками кредитных организаций, мошенники пытаются выведать у людей на другом конце провода секретную информацию, с помощью которой легко можно похитить деньги с карты жертвы. В Отделении Банка России по Чеченской Республике рассказали, как защитить свои средства от аферистов.

**Кто на проводе: банк или мошенники?**

В условиях роста активности мошенников излишняя бдительность не помешает. При малейших сомнениях, чтобы не стать жертвой обмана, не спешите отвечать на вопросы собеседника. Лучше уточните его фамилию, имя, отчество, спросите, в каком подразделении он работает. Затем положите трубку и вручную наберите номер горячей линии банка, который указан на оборотной стороне вашей карты. Так вы узнаете, действительно ли вам звонили из кредитной организации и есть ли реальные проблемы с вашей картой. Важно помнить, что, совершая обратный звонок по входящему номеру, вы рискуете вновь попасть на телефон, с которого звонили мошенники.

**Под угрозой – доверчивые граждане**

Мошенники не стоят на месте, постоянно совершенствуя свое «мастерство». Чтобы жертва поверила в то, что она действительно разговаривает с банковским работником, злоумышленники включают фоном звуки колл-центра, переключают собеседника с одного оператора на другого.

Будучи тонкими психологами, киберпреступники запугивают свою жертву, говоря о том, что в момент разговора якобы кто-то предпринимает попытку списания денег с карты. Чтобы остановить операцию, человека просят сообщить персональные данные или платежные реквизиты, с помощью которых мошенники легко могут завладеть чужими средствами.

**Наши данные – не тайна?**

Казалось бы, откуда злоумышленникам знать номер телефона, фамилию, имя, отчество своей жертвы? На самом деле, источником информации могут служить социальные сети, в которых люди излишне выставляют свою жизнь напоказ, что на руку преступникам. Не исключены и хищения личных данных либо утечки информации из самих банков или других организаций, в которых люди оставляли свои персональные данные.

**Как защитить свои средства?**

Закон на стороне пострадавшего, но важно помнить, что в случаях, когда человек сам сообщил мошенникам секретную информацию, рассчитывать на возмещение ущерба через банк не придется. Чтобы не стать такой жертвой, не переходите по ссылкам из сообщений «от банка», не перезванивайте и не отправляйте СМС на незнакомые номера. Помните, что при обнаружении подозрительной операции банк заблокирует на срок до двух суток. Этого времени достаточно, чтобы все обдумать и принять решение. А еще настоящий сотрудник банка не будет спрашивать личные данные, реквизиты карты и секретную информацию. Называть кодовое слово можно только в том случае, если вы сами звоните на горячую линию банка.