**Звонок от банка или мошенника?**

**В последнее время активизировались телефонные мошенники, выдающие себя за представителей банков. При этом номера телефонов, с которых они звонят, маскируются под официальные номера коммерческих банков.**

Чтобы избежать финансовых потерь, необходимо соблюдать следующее правило. Даже если на телефоне высветился знакомый номер банка, узнайте имя и фамилию звонящего, название банка и подразделения, где он работает, а затем положите трубку. После этого позвоните в банк, **вручную набрав** номер горячей линии, который указан на обратной стороне банковской карты или на официальном сайте банка. Попросите перевести ваш звонок на того сотрудника, который вам звонил.

Если такая предосторожность кажется вам излишней, то имейте в виду, что современное программное обеспечение позволяет скрыть настоящий номер звонящего, отображая на экране вашего телефона официальный номер банка. Злоумышленник может знать ваши имя и фамилию, номер карты и срок ее действия. Эту информацию мошенники получают из социальных сетей и с помощью вредоносных программ.

Цель звонка преступника – получить секретные данные, которые можете предоставить только вы: CVC/CVV-код на обратной стороне карты, одноразовые коды из СМС, ПИН-коды, кодовые слова. Чаще всего для этого создается видимость опасности, которая угрожает средствам на вашей карте. Например, по карте якобы совершается попытка провести операцию по списанию денег. Попавшись на эту уловку, в итоге человек действительно теряет свои сбережения.

Важно помнить: если банк выявил подозрительную транзакцию по вашей карте, он немедленно приостановит ее на срок до двух суток. За это время вы спокойно проверите всю информацию и либо подтвердите эту операцию банку, либо отмените ее. Однако если мошенникам удалось получить доступ к деньгам на вашем счете, потому что вы сами сообщили преступникам секретную информацию, которую нельзя разглашать, возместить утраченные средства через банк не получится.

«Не сообщайте никому следующие реквизиты платежной карты: ПИН-код, трехзначные CVV и CVC-коды, срок действия платежной карты, коды из СМС, а также информацию, необходимую для доступа в мобильный и Интернет-банк, – напоминает начальник Управления платежных систем и расчетов Северо-Западного главного управления Банка России Ирина Поздеева. – Важно знать, что коды и пароли генерируются и проверяются программным обеспечением банков автоматически без участия человека. Служащие банка не имеют права запрашивать коды и пароли клиента».

Если вам звонили злоумышленники, сообщите об этом звонке в ваш банк и в Банк России - через интернет-приемную или по телефону «горячей линии» 8-800-300-3000.