**Звонят «из банка»? Не доверять, а проверять!**

**Чужие деньги всегда были и остаются лакомым кусочком для мошенников: сколько веков люди стараются накопить и приумножить, столько же времени и преступники находят способы обмануть и присвоить.**

От действий мошенников страдают и куряне. Хитрость и изобретательность злоумышленников не дает времени сообразить, что происходит, и люди расстаются с деньгами, сами того не подозревая. Многие знают, что отвечать на звонки с незнакомых телефонных номеров и смс нельзя. Но как быть, если человек видит на экране телефона реальный номер горячей линии банка, общается с представителем колл-центра и… лишается денег? Разбираемся, как такое возможно и как обезопасить себя, вместе с управляющим курским отделением Банка России Евгением Овсянниковым.

**- Евгений Викторович, в последнее время мошенники звонят с номеров горячих линий банков, представляются сотрудниками и пытаются узнать у курян информацию. Те, кто добросовестно отвечает им, лишаются денег. Как вообще мошенники это делают?**

- К сожалению, сейчас появились такие технологии, когда мошенники, используя специальное программное обеспечение, маскируют свой номер под официальный номер банка.

«Лжебанкиры» хорошо подготовлены – они обращаются к собеседнику по имени и отчеству, часто знают фамилию, а иногда даже номер и срок действия карты.

**- Откуда они берут эту информацию? Им кто-то ее сообщает?**

- По анализу данных, которые чаще всего называют мошенники в разговоре с жертвой можно сделать вывод, что сведения они зачастую находят в открытых источниках. В том числе – в социальных сетях, а также с помощью фишинга в Интернете. Их расчет прост: человек не должен сомневаться и сам доверит звонящему максимум нужной информации. Мошенники – хорошие психологи, они знают, как создать ощущение реальности происходящего.

**- Можно выделись какие-то приемы, которыми пользуются преступники? Может быть, они помогут курянам быть более внимательными…**

- Начнем с того, что обычно такие звонки раздаются поздно вечером, ночью или ранним утром в выходные. Чаще всего в это время человек спит или находится в рассредоточенном состоянии и не может быстро сориентироваться. И тут якобы сотрудник банка сообщает о подозрительной операции и просит клиента немедленно предпринять определенные действия. При этом злоумышленники владеют профессиональной терминологией, говорят быстро, уверенно и иногда используют фоновые звуки, чтобы создать иллюзию работы колл-центра. Они пугают клиента тем, что по карте совершаются подозрительные операции, требуют срочно сообщить одноразовый пароль из СМС-сообщения и другие секретные данные, чтобы остановить списание средств. А если человек отказывается их назвать, начинает размышлять – мошенники нагнетают обстановку, пугать непоправимыми последствиями. Сложно в такой ситуации не потерять бдительность… А как только преступники узнают нужную информацию, для них открывается доступ к деньгам жертвы.

**- Схема понятна. Как действовать человеку, чтобы не лишиться денег и не выдать преступникам конфиденциальной информации??**

- Для начала при подобном звонке обязательно проверьте, действительно ли это сотрудник банка: спросите его имя и фамилию, название подразделения и ответьте, что перезвоните позже. Сразу же прекратите звонок и положите трубку! После этого позвоните по официальному номеру банка и попросите соединить с сотрудником, который вам звонил.

Чтобы вновь не попасть на линию к мошенникам, номер горячей линии банка наберите вручную. Он находится на обратной стороне банковской карты или на официальном сайте банка.

Никогда не перезванивайте и не отправляйте СМС на незнакомые номера! Даже если вы уверены, что сообщение прислал банк, не переходите по содержащимся в нем ссылкам. Во всех ситуациях, так или иначе затрагивающих вопросы безопасности ваших денег, лучше звонить в банк по официальному номеру и задавать вопросы.

Обязательно успокойтесь: не паникуйте и не спешите, даже если вам сообщают, что обнаружена подозрительная операция и деньги вот-вот спишут. По закону при обнаружении подозрительной транзакции банк сразу же останавливает ее на срок до двух суток – за это время вы подтверждаете или отменяете операцию. На решение вам дадут не пару минут, а 48 часов, чтобы можно было разобраться, что происходит и самому связаться с банком. Если же вы ничего не сделаете, то операция пройдет только через двое суток, когда банк автоматически снимет блокировку.

Никогда, никому и ни при каких условиях не сообщайте личные данные, реквизиты карты и секретную информацию: ПИН-код, CVC/CVV-код на обратной стороне карты и особенно коды из СМС. А «кодовое слово» можно называть только в том случае, если вы сами звоните на горячую линию банка. Если клиент сообщает преступникам секретную информацию сам, украденные деньги банк вернуть не сможет.

А если подводить итог всему сказанному выше, то правила таковы: при подозрительных смс и звонках не паникуйте, прекращайте общение, набирайте вручную номер горячей линии банка и выясняйте, что происходит. Даже если такая бдительность кажется вам чрезмерной – поверьте: лучше перестраховаться!