Приложение

Популярность банковских карт растет с каждым годом. Это неудивительно: оплата товаров и услуг картой удобна, не надо носить с собой крупные суммы наличных, возможен круглосуточный доступ к собственным средствам. Банковские карты прочно вошли в нашу повседневную жизнь, однако при их использовании нужно соблюдать простые, но очень важные меры безопасности. Ведь в последнее время участились случаи sms-мошенничества. Схема довольна проста: на мобильный телефон приходит сообщение о том, что ваша банковская карта заблокирована. Чтобы ее разблокировать, вам предлагают ввести какую-то информацию в ответном сообщении или перезвонить по указанному номеру. Человек, растерявшись, сообщает мошенникам персональные данные или информацию о банковской карте, в результате чего теряет свои деньги.

Расчет мошенников прост. Большинство пользователей платежных карт для собственного удобства подключают «мобильный банк». Эта услуга действительно полезна, так как позволяет в режиме реального времени узнавать, что происходит с вашим счетом – при оплате покупок, поступлении денег на него и т.п. Пользуясь «мобильным банком», человек привыкает, что постоянно получает подтверждение своих действий посредством sms. Обнаружив сообщение о блокировке карты, многие клиенты порой даже не смотрят на номер, с которого оно поступило.

Чтобы избежать непредвиденных ситуаций, важно следовать правилам:

1. Для связи с банком, выпустившим карту, используйте только те контактные данные, которые указаны в документах, выданных в самой кредитной организации, или на оборотной стороне карты. Кстати, рекомендуется записать номер телефона банка, чтобы он всегда был под рукой. Если же вы получили сообщение или звонок с любого другого номера – не перезванивайте, не переходите по ссылкам, не сообщайте никакую информацию – даже фамилию и имя.
2. Если у вас возникли сомнения, позвоните по номеру горячей линии вашего банка (он должен быть указан на оборотной стороне карты) и убедитесь, что с карточным счетом все в порядке.
3. Никогда не сообщайте ПИН-код карты, код CVV2/CVC2 (три цифры на обратной стороне карты), а также код-подтверждение из sms от банка даже его сотрудникам. Если вы подозреваете, что кто-то все же узнал коды карты или ваши персональные данные, которые могут позволить мошенникам снять наличные или расплатиться вашей картой, немедленно обратитесь в банк, ее эмитировавший. Так же надо поступить и в случае утери или кражи карты. Помните, что в договоре с кредитной организацией, как правило, прописано, что деньги, списанные со счета в результате несанкционированного использования вашей платежной карты до момента уведомления об этом банка, не возмещаются.
4. Не переводите и не зачисляйте деньги в ответ на просьбы, поступающие с неизвестных номеров, а если просьба исходит якобы от родственника или друга, но с незнакомого номера, позвоните ему на известный вам номер и уточните, верна ли информация.
5. Не набирайте на мобильном устройстве цифровые команды, назначение которых вам неизвестно.
6. При потере мобильного телефона срочно обратитесь к оператору сотовой связи для блокировки номера и в контактный центр банка для приостановления или отключения «мобильного банка». Если вы решили отключить сервис от утерянного номера, обратитесь в банк с заявлением о подключении «мобильного банка» к другому, актуальному номеру.
7. Установите на свой мобильный телефон антивирус и регулярно его обновляйте. Это может защитить вас от вредоносного программного обеспечения.