**Банковская карта: как обезопасить себя**

**и не стать жертвой мошенников**

В современном мире пользоваться пластиковыми картами, как кредитными, так и дебетовыми, очень удобно. Но там, где есть деньги, всегда есть мошенники, которые, пользуясь нашим доверием, похищают деньги.

Сотрудники службы безопасности СКБ-банка рассказали, как пользоваться банковскими картами, чтобы не стать жертвой мошенников.

Трудно поспорить с тем, что банковская карта – это очень удобно. У карты есть и процент на остаток, и кэшбэк (возврат наличных от покупок), к тому же, она гораздо компактнее и удобнее в использовании, чем наличные. Считается, что пластиковая карточка потенциально более безопасна, так как без знания пин-кода злоумышленники не смогут ею воспользоваться. Но это не совсем так.

Скимминг, фишинг, фарминг – все эти термины означают различные способы хищения средств с банковских карт без ведома их законного владельца. Вариантов очень много.

Для копирования магнитной полосы мошенники часто используют специальные накладки на клавиатуру банкомата или скрытые камеры. Но зачастую люди сами необдуманно делятся данными своей банковской карты. Чтобы снять деньги с чужой пластиковой карты, злоумышленникам достаточно знать номер карты (16 цифр на лицевой стороне) и CVV2-код (последние три цифры с обратной стороны карты). Схемы выманивания этих сведений просты и рассчитаны, в основном, на доверие людей. Вот основные из них.

**СМС о выигрыше.** Часто на телефон может прийти смс о том, что вы стали победителем розыгрыша. Для получения приза требуется перезвонить по указанному номеру телефона. При звонке человека просят сообщить номер и код карты, чтобы перевести сумму «вымышленного» выигрыша. Жертва обмана сообщает личные данные мошенникам и прощается со всеми деньгами, которые есть на карте.

**Звонок о блокировке карты.** При таком способе клиенту поступает звонок от мошенника, сообщается, что «ваша карта заблокирована», но при этом на экране отображается номер телефона вашего банка. Для «разблокировки» карты понадобится информация по карте: номер и CVV2-код.

**Психологические приемы.** Зачастую мошенники пользуются психологическим давлением, переводя жертву в стрессовое состояние. Варианты могут быть разными, но главная цель – сообщить, что ваши деньги в опасности.

Прежде всего, нужно соблюдать нехитрые способы безопасности. Это позволит вам сохранить свои сбережения.

Помните о том, что отдать персональные сведения о карте или кредитке посторонним – это все равно, что подарить свой кошелек. Ни в коем случае не оставляйте карты без присмотра и не записывайте пин-код в доступных местах. Ни работники банка, выдавшего карту, ни обслуживающий персонал банкомата не вправе требовать таких данных.

Если вы храните на карте достаточно большую сумму, установите лимиты на единовременное снятие и на дневной оборот наличных. Будет полезным подключить SMS-оповещение к вашей карте. Услуга стоит недорого и поможет держать ваш электронный кошелек под контролем. Вы сразу же узнаете о том, что по вашей карте была совершена незаконная операция.

Одно из важных правил – никогда не сообщайте CVV2-код, указанный на оборотной стороне карты.

В интернете также стоит соблюдать осторожность: не пересылайте данные карты по электронной почте и не оставляйте логины и пароли к своему личному кабинету в онлайн-банкинге на компьютере. При оплате через интернет пользуйтесь только проверенными сайтами, а также обращайте внимание на строку браузера (она должна начинаться так: https://, где «s» обозначает, что ваши данные будут передаваться по защищенному каналу связи). Советую уточнить, используют ли в вашем банке специальный сервис 3D-Secure. Он позволяет совершать покупки в интернет-магазинах через защищенное соединение. Для подтверждения операции вам должны высылать на телефон одноразовый пароль.

Если ваша карта с магнитной полосой, лучше получите новую карту с чипом, так как она надежнее.

Старайтесь снимать наличные в банкоматах своего банка и не пользоваться банкоматами в мелких магазинах и аптеках. Обязательно проверьте устройство. Если заметите что-то подозрительное, позвоните в банк. Для удобства запишите номер call-центра банка в свой мобильный телефон. Если карта будет потеряна или украдена, то нужно сразу же позвонить в банк и заблокировать ее.

В случае, если кто-то все же стал жертвой мошенников, нужно сразу же обратиться в банк и полицию с заявлением об отмене операций и возврате денежных средств.

Банковская карта – это действительно удобно, но обязательно нужно соблюдать безопасность, чтобы не потерять свои накопления.

ПАО «СКБ-банк»

тел. 88001000600