Статья № 3

Платежная карта – способ банковского обслуживания

В предыдущих публикациях наши читатели узнали, какие бывают банковские карты, какие операции можно совершать с их помощью, как контролировать расходы по карте. Сегодня мы продолжаем публиковать интервью управляющего Отделением по Курской области Главного управления Банка России по Центральному федеральному округу Овсянникова Евгения Викторовича.

- Евгений Викторович, давайте поговорим о вопросах безопасности.

Существует несколько правил, позволяющих обезопасить держателей карт от злоумышленников.

Во-первых, нельзя сообщать ПИН-код, а также CVV - код (это три или четыре цифры, расположенные на оборотной стороне вашей карты) третьим лицам, особенно сотрудникам кредитных организаций (в том числе службе безопасности и прочим службам), и хорошим знакомым, даже родственникам!

Во-вторых, свой ПИН-код нужно запомнить, а не писать его на своей карте – это самая распространенная ошибка забывчивых держателей карт. Главное, ни в коем случае не хранить записанный ПИН-код вместе с картой, например, в кошельке или бумажнике. Можно придумать способ хранить ПИН отдельно от самой карты в недоступном для других месте. Помните, что в случае утери или кражи карты и ПИН-кода злоумышленники получат полный доступ к вашим денежным средствам.

В-третьих, никогда не передавайте карту посторонним людям. Очень важно подключить электронную услугу СМС-оповещения о проведенных операциях.

Нельзя отвечать на электронные письма или СМС-сообщения, которые приходят якобы от вашей кредитной организации или от Центрального банка Российской Федерации, в которых предлагается предоставить свои персональные данные или следовать по указанным ссылкам. В этой связи напомню, что **Центральный банк Российской Федерации (Банк России) не обслуживает физических лиц.**

- А что делать, если карта утеряна?

Если вы потеряли карту, или же у вас появились опасения, что ПИН-код стал известен кому-то, немедленно обратитесь в банк с целью

блокировки вашей карты до выдачи новой карты или смены ПИН-кода, подтвердив свое сообщение письменным заявлением.

Для проведения операций через банкомат лучше выбирать безопасные места (подразделения банков, крупные торговые комплексы и т.п.). Не используйте офисы организаций, которые требуют ввода ПИН-кода для доступа в помещение, где расположен банкомат.

Перед началом работы с устройством осмотрите банкомат на предмет повреждений, заметных неисправностей, дополнительных устройств на клавиатуре и отверстии для приема карт. Если что-то показалось вам подозрительным – воздержитесь от использования этого банкомата и сообщите о своих опасениях в банк по телефону, указанному на банкомате. Никогда не совершайте операции в присутствии подозрительных лиц.

Обязательно обращайте внимание, присутствует ли на банкомате логотип платежной системы, указанный на вашей банковской карте (Visa, MasterCard, МИР и т.п.). Всегда, вводя ПИН-код, прикрывайте клавиатуру свободной рукой, чтобы его не смогли увидеть не только люди, находящиеся рядом, но и камеры. Будьте внимательны и не допускайте ошибок при вводе ПИН-кода, поскольку после трех неверных попыток ваша карта может быть временно заблокирована (обычно до следующего дня).

Если банкомат «зависает» или самопроизвольно перегружается, нажмите кнопку «Отмена» и дождитесь возврата карты. Если банкомат ее не возвращает, не отходя далеко от банкомата, немедленно позвоните по телефону, указанному на банкомате, и следуйте инструкциям сотрудника банка, главное – **не сообщайте никому ПИН-код карты.**

Также важно знать, что мошенники могут по телефону представиться вашими родственниками, случайно попавшими в беду, и требовать срочно перевести им деньги на незнакомые счета или номера мобильных телефонов. В таких ситуациях следует сохранять спокойствие и благоразумие и не идти к ближайшему банкомату, чтобы совершить перевод, а спокойно позвонить своему родственнику или лицу, которым представились мошенники или от имени которого они звонили. Такие звонки всегда происходят с незнакомых вам номеров с просьбой не перезванивать на номер родственника по какой-либо «уважительной» причине. Стоит также отметить, что если вы переведете таким образом денежные средства, это будет обычный денежный перевод, выполненный вами добровольно, и завести уголовное дело будет достаточно сложно, так как операция с использованием карты и вводом ПИН-кода признается совершенной держателем карты.

Сейчас распространился вид мошенничества с восстановлением данных личного кабинета через СМС-сообщения. Вам могут позвонить и представиться сотрудником банка или другим лицом, которое сообщит вам о

поступлении денежных средств на ваш счет, и для того, чтобы перевод состоялся, вам необходимо сообщить код, который придет вам в СМС-сообщении. После того как вы скажете код, злоумышленник сможет перевести **ваши деньги на свой счет**. Многие действия мошенникам приходится проделывать повторно под предлогом, что код не сработал и придет другой, это уже коды на разрешение перевода. Поэтому повторяю, будьте бдительными и не передавайте информацию никому, даже сотрудникам банка.

- Как правильно хранить платежную карту?

Беречь карту нужно так же, как берегут наличные деньги: от механических повреждений, от воздействия влаги. Держите карту вдали от электроприборов и электромагнитных излучений. Помните, что обычно перевыпуск карты по вине клиента является платным (около 500 рублей).

Обязательно распишитесь на оборотной стороне вашей карты. Перепишите и храните в недоступном месте реквизиты карты и телефон кредитной организации, размещенный на карте или в договоре, заключенном с кредитной организацией, они пригодятся вам в случае потери или кражи банковской карты, чтобы своевременно ее заблокировать.

Если карту украли, следует срочно связаться со службой клиентской поддержки вашего банка по телефону или отправить сообщение по «Мобильному банку» (если такая услуга подключена), проинформировать о сложившейся ситуации, попросить заблокировать карту и сделать заявку на ее перевыпуск. Для более оперативной связи с банком рекомендуется всегда иметь при себе телефон службы клиентской поддержки, а также сохраненное СМС-сообщение с текстом-командой для блокирования карты. Обязательно в кратчайшие сроки подтвердите свой звонок письменным заявлением в офисе банка.