Осторожно, кибермошенники!

Банковские карты – удобное современное средство платежа. Количество людей, пользующихся банковскими картами, и объемы операций с использованием данного платежного инструмента постоянно растут. Не дремлют и мошенники. Только за 2016 год с банковских карточек россиян ими было украдено более 1 млрд рублей.

Простейшие правила кибербезопасности следует помнить и соблюдать всем без исключения: владельцам платежных карт и электронных кошельков, пользователям систем интерет-банкинга и систем дистанционного банковского обслуживания. Преступники всегда делают ставку на нашу невнимательность, доверчивость, легкомыслие.

Вот несколько реальных историй, произошедших в нашем регионе.

В одну из рязанских кредитных организаций обратился клиент с жалобой на неправомерное списание с его банковской карты денежных средств в сумме, эквивалентной приблизительно 40 евро. Клиент узнал о факте списания денежных средств незамедлительно, так как использовал предоставляемый банком сервис информирования по SMS об имевших место операциях. По факту списания денежных средств через кредитную организацию подготовлены запросы в платежную систему на опротестование транзакций, которые были удовлетворены. По мнению клиента, неправомерное списание денежных средств произошло вследствие использования реквизитов банковской карты на сомнительном сайте в сети Интернет. «Во всех случаях следует внимательно относиться к тому, на каких сайтах публикуются данные платежной карты. Если имеются сомнения в надежности сайта, лучше воздержаться от указания на нем реквизитов своей банковской карты», - напоминает управляющий Отделением по Рязанской области ГУ Банка России по Центральному федеральному округу Маргарита Одинцова.

Другой случай является примером крайне неаккуратного обращения со своей банковской картой, в результате чего ее владелец потерял более 10 тыс. рублей. Как выяснилось после обращения владельца карты в банк, данные своей карты в виде фотографий лицевой и оборотной сторон незадолго до хищения он направил по электронной почте близкому родственнику. «Никогда не следует сообщать данные своей карты (ее номер, пин-код, срок действия, код CVC/CVC2, кодовое слово и т.д.), даже близким родственникам, особенно с использованием электронных средств связи: эти данные могут легко оказаться в руках мошенников», - рекомендует Маргарита Одинцова.

Потенциальными жертвами злоумышленников иногда становятся также и юридические лица, которые используют дистанционный доступ к своим банковским счетам. Так, один из рязанских предпринимателей в начале марта 2016 года мог потерять около полумиллиона рублей из-за таких мошеннических действий. Злоумышленники, внедрив троянскую программу на компьютер предпринимателя, удаленно и скрытно сформировали платежное поручение о переводе денежных средств. Фиктивный платеж был остановлен операционистом банка в ходе дополнительного контроля, деньги возвращены владельцу.

Чтобы не допустить крупных финансовых потерь при использовании программ дистанционного доступа к счету, надо соблюдать базовые требования безопасности: применять только лицензионное программное обеспечение, актуальные антивирусные средства, исключить неконтролируемый доступ к компьютеру. Полный перечень необходимых мер безопасности, как правило, публикуется банками на своих сайтах и доводится до клиентов при заключении договора на банковское обслуживание, - советуют в Отделении по Рязанской области ГУ Банка России по Центральному федеральному округу.