Актуальные угрозы при использовании пластиковых карт

1. СМС - мошенничество

Мошенники рассылают СМС-сообщения о блокировании карты, приостановке обслуживания по карте, изменении ПИН-кода, окончании срока действия карты и т.д. с рекомендациями направить информацию о реквизитах пластиковой карты. Банк никогда не осуществляет отправку СМС-сообщений с целью получения реквизитов Вашей карты или какой- либо другой информации о клиенте.

2. Мошенничество через e-mail

Под видом сообщений от имени Банка мошенники могут проводить e-mail-рассылки с целью заманить получателя сообщения на сайт-ловушку и под различными предлогами получить его персональные данные (кодовое слово банковской карты, номер банковской карты, ПИН-код, CVV-код, идентификатор и пароль для входа в интернет-банк и другую информацию). Банк никогда не рассылает сообщений с просьбой подтвердить, обновить или предоставить персональные данные.

3. Мошенничество через телефонные звонки

Мошенники могут позвонить Вам и, представившись сотрудниками Банка, попросить Вас сообщить полный номер карты, срок её действия, ПИН-код и другие реквизиты. Никогда не называйте реквизиты Вашей карты по телефону, даже если уверены, что разговариваете с сотрудником Банка. При необходимости можно назвать только номер карты.

4. Мошенничество при заказе товаров и услуг через интернет-магазин

Если для совершения покупки в интернет-магазине Вас просят ввести ПИН-код, игнорируйте эту просьбу, так как это уловки мошенников. Для оплаты покупок в сети Интернет рекомендуется использовать виртуальную банковскую карту на определенную сумму и определенное количество покупок. Виртуальную банковскую карту можно заказать через систему интернет-банк.

5. Мошенничество при расчётах пластиковой картой в магазине

При расчетах пластиковой картой за покупки или услуги сотрудники торговой точки (кафе, ресторана, медицинского учреждения, салона красоты и т.д.) могут скопировать реквизиты Вашей пластиковой карты и в дальнейшем, сделав копию Вашей карты, воспользоваться Вашим картсчетом. Требуйте проведения операций с Вашей картой только в Вашем присутствии, не позволяйте уносить карту из поля Вашего зрения.

6. Установка нелегальных считывающих устройств на банкоматах и использование нелегальных мобильных считывающих устройств

Для получения конфиденциальной информации о Вашей карте мошенники могут установить считывающие устройства над ПИН-клавиатурой и на устройство для приёма карты в банкомате. При обнаружении подозрительных устройств в указанных местах не проводите операции с пластиковыми картами в данном банкомате.

Мошенники могут использовать нелегальные мобильные устройства для считывания данных с карт, поддерживающих технологию бесконтактной оплаты. Позаботьтесь о недоступности Вашей бесконтактной карты для посторонних устройств и подключите услугу СМС-информирования об операциях по бесконтактной карте. Это позволит Вам оперативно получать информацию обо всех операциях, совершаемых по Вашей карте.