Мошенничество с использованием банковских карт

Способы минимизации рисков

- пользоваться только банкоматами, установленными в безопасных местах;
- внимательно осматривать банкомат, перед его использованием;
- закрывать клавиатуру при вводе пин-кода;
- оформить услугу SMS-оповещения о проведенных операциях по карте;
- оформить услугу SMS-оповещения о проведенных операциях по карте;
- не хранить пин-код вместе с картой не сообщать по мобильным или стационарным телефонам реквизиты карты и ее пин-код;
- блокировать карту немедленно в случае утери/хищения)

- Скимминг* (от англ. skim - снимать сливки)— установка на банкоматы нештатного оборудования (скиммеров), которое позволяет фиксировать данные банковской карты (информацию с магнитной полосы банковской карты и вводимый пин-код) для последующего хищения денежных средств со счета банковской карты.

Мошенникам нужны:

- Номер карты
- Имя владельца
- Срок действия
- Номер CVC или CVV

Как и где происходит кража данных

- В банкомате. Мошенники могут установить скиммер и видеокамеру
- В социальных сетях. Мошенник может попросить у Вас прислать данные карты
- В кафе или магазине сотрудник злоумышленник может сфотографировать карту

Что делать, если с карты списали деньги

- Позвонить в банк и заблокировать карту;
- Запросить выписку по счету и написать заявление о несогласии с операцией;
- Обратиться в полицию

Примеры мошенничеств с использованием банковских карт

Тревожное смс-сообщение или звонок от родственника

- С незнакомого номера вам пишет или звонит якобы родственник и говорит, что попал в беду и ему срочно нужны деньги, но времени объяснять ситуацию у него нет. В таких сообщениях часто манипулируют срочностью ситуации, и присылают их в крайне неудобное время, например, ночью.
- Не спешите переводить деньги. Попытайтесь выяснить детали — обычно долгие разговоры не входят в планы злоумышленников. Если выяснить ничего толком не удалось, перезвоните родственнику, от имени которого обращаются, чтобы убедиться, он ли вам звонит/пишет.

Сообщение «от банка»

- С незнакомого номера приходит смс-сообщение, что ваша карта заблокирована. В смс указан номер, по которому нужно позвонить для уточнения деталей. Позвонив, вы попадете в фальшивую службу безопасности банка, где вас будут убеждать сообщить данные карты или подойти к ближайшему банкомату и произвести операции. Выполнив указания злоумышленников, вы откроете им доступ к карте и они украдут ваши деньги.
- Не перезванивайте — сперва выясните, действительно ли звонили из вашего банка. Настоящие банки обычно присылают уведомления с одного и того же номера. Кроме того, на вашей карте указан телефонный номер для связи с банком — позвоните по нему и уточните, заблокирована ли она. Или обратитесь к сотрудникам ближайшего отделения банка.

Звонок из госучреждения

- Вам звонят люди и представляются сотрудниками Банка России, прокуратуры, суда, Министерства здравоохранения, Министерства финансов и других учреждений. Они сообщают, например, о положенном возмещении ущерба от действий мошенников: о компенсации за купленные медицинские товары или услуги экстрасенсов. Если для получения обещанной компенсации «сотрудник» попросит вас что-то оплатить (подоходный налог, налог на прибыль, банковский сбор, обязательную страховку, госпошлину, комиссию за перевод денег), а тем более попросит предоставить паспортные данные или банковские реквизиты, это — телефонный мошенник.
- Не следуйте указаниям и ничего не оплачивайте. Не предоставляйте личную информацию, у настоящих сотрудников она уже есть.