**Как распознать телефонного злоумышленника?**

Практически каждый день многие из нас используют пластиковые карты, мобильные телефоны, компьютеры.

Обмануть или взломать банковскую систему безопасности достаточно сложно, поэтому преступники стараются любыми способами выманить информацию о карте у самого держателя. Для достижения своей цели они используют все доступные ресурсы – телефон, интернет-сайты, онлайн-банк, мобильный банк и прочие каналы.

Есть несколько типичных способов.

По телефону. Данный вид хищения имеет много вариантов, которые объединяет то, что владельцу карты звонят с незнакомого номера и под любым предлогом просят сообщить реквизиты банковской карты.

Как правило, звонящие представляются сотрудниками службы безопасности банка. Лже банковский работник извещает клиента о том, что по его карте совершена сомнительная операция, либо его карту пытались взломать. После чего предлагает уточнить данные для исправления ситуации.

Отличает звонящих уверенное поведение, хорошо поставленный голос, умение быстро и убедительно ответить на любой вопрос обеспокоенного клиента.

Через смс-сообщения. Данная схема схожа с предыдущим способом. Разница в том, что ложная информация приходит в тексте СМС-сообщения. Рассылка осуществляется с незнакомого номера с «подписью» известной компанией.

Типичный пример подобного сообщения: «Ваша карта заблокирована. Перезвоните по номеру +7926ХХХХХХХ. Ваш банк». Если клиент не реагирует, то преступники могут прислать повторное СМС с угрозой взыскания штрафа или комиссии. Перезвонившего просят сообщить данные карты, провести манипуляции в банкомате или интернет-банке.

Хищения с переводом денег на карту. Способ незаконного обогащения – убедить человека в том, что он должен перевести деньги самостоятельно. Злоумышленники предлагают приобрести товары по выгодной цене и требуют перечисления аванса или всей суммы.

Распространенной схемой аферистов также является «помощь родным». Данный способ чаще всего применяется в отношении пожилых людей, которым звонят и сообщают о том, что их близкие попали в беду. Мошенники представляются сотрудниками правоохранительных органов или медицинскими работниками. Они настоятельно требуют перевести деньги, угрожая необратимыми последствиями для жизни и здоровья близких.

Чтобы обезопасить себя от действий мошенников, необходимо придерживаться следующих правил:

- не сообщать конфиденциальные данные карты (срок действия, CVV-код, ПИН-код);

- подключить услугу СМС-уведомлений для контроля за счетом;

- ПИН-код хранить отдельно от карточки, прикрывать рукой клавиатуру банкомата или терминала в момент его ввода;

- никогда никому не сообщать код из СМС для подтверждения операции (сотрудники банка не вправе запрашивать данную информацию);

- немедленно блокировать карту в случае утраты, кражи или захвата ее банкоматом, а также при утере телефона с привязанным номером.

В случае незаконного списания денежных средств с банковской карты необходимо незамедлительно обратиться в отделение банка для блокировки карты и составления заявления о несогласии с конкретной расходной операцией.

Кроме того, по всем фактам хищения денежных средств необходимо обращаться в территориальный орган внутренних дел.

Старший помощник прокурора города Кремс Д.К.