Мошенничество с банковскими картами, способы обмана

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.

По телефону: данный вид мошенничества имеет множество вариаций, которые объединяет то, что владельцу карты звонят с незнакомого номера и под любым предлогом просят сообщить её реквизиты.

В большинстве случаев злоумышленники используют схему звонок из службы безопасности банка. Фальшивый «сотрудник» извещает клиента о том, что его карту пытались взломать и просит уточнить данные для исправления ситуации. Телефонные мошенники всегда говорят уверенно, имеют хорошо поставленный голос, а на любой вопрос клиента имеют заранее подготовленный ответ.

Через СМС эта схема имеет много общего с предыдущим способом. Разница заключается в том, что ложная информация приходит в тексте СМС-сообщения. Рассылка осуществляется с незнакомого номера, но мошенники подписываются известной компанией. Распространённый пример подобных фейковых сообщений: «Ваша карта заблокирована. Перезвоните по номеру +7926XXXXXXX. Ваш Сбербанк.» 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.

Через мобильный банк, услуга «Мобильный банк» позволяет совершать операции с помощью СМС-команд. Чтобы перевести средства другому клиенту, достаточно отправить сообщение на короткий номер банка с того телефона, который привязан к карте. Мошенники используют данную опцию в следующих случаях: Телефон был утерян владельцем. До момента блокировки SIM-карты любой человек может списать деньги с карточки с помощью СМС-команд, перечень которых размещён на сайте любого банка. Клиент отказался от услуг конкретного сотового оператора и не отключил мобильный банк. В этом случае номер телефона попадёт в руки нового абонента, который может оказаться мошенником и списывать деньги посредством СМС-команд. Благодаря использованию мобильного банка злоумышленник также легко вычислит, в какой организации владелец телефона открыл карту.

Самый простой способ незаконного обогащения — это убедить гражданина в том, что он должен перевести деньги самостоятельно. Злоумышленники предлагают приобрести товары по выгодной цене и требуют перечисления аванса или всей суммы. Некоторые мошенники выступают в роли фиктивных компаний, которые предлагают удалённую работу в интернете с хорошим заработком. Соискателю необходимо лишь

подтвердить серьёзность своих намерений и перевести определённую сумму на счёт или карту работодателя.

Распространённой 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.

Что делать, если с карты украли деньги?

Чтобы обезопасить себя от действий мошенников, необходимо придерживаться следующих рекомендаций: не сообщать конфиденциальные данные карты третьим лицам (срок, CVV-код и ПИН-код); подключить услугу СМС-уведомлений для контроля за счётом; ПИН-код хранить отдельно от карточки и прикрывать рукой клавиатуру банкомата или терминала в момент его ввода; установить расходные лимиты в интернет-банке или мобильном приложении; никогда никому не сообщать код из СМС для подтверждения операции, которую клиент не совершал (сотрудники банка не вправе запрашивать данную информацию); немедленно блокировать карту в случае утраты, кражи или захвата её банкоматом, а также при утере телефона с привязанным номером.

Ежедневно злоумышленники изобретают новые способы хищения средств с банковских карт, поэтому невозможно предугадать все сценарии развития событий.

Однако при соблюдении указанных элементарных мер безопасности любой пользователь сможет предотвратить нанесение ущерба от действий м о ш е н н и к о в !

помощник прокурора
Новосибирского района
юрист 3 класса
Архипова М.В.