МОШЕННИЧЕСТВО В ФИНАНСОВОЙ СФЕРЕ

Прокуратура Ленинского района г. Иркутска

2024 г.

Виды мошеннических действий в финансовой сфере.

! Способы мошенничества с банковскими картами

Махинации с банковскими картами осуществляются различными способами: от самого простого варианта в виде подсматривания пин-кода или кражи карты до самого сложного, связанного с хакерскими уловками.

! По телефону, через смс

Сейчас почти все банковские карты привязываются к сим-картам (к номерам телефонов). Это создает опасность в случае утери сим-карты, нашедший ее человек может получить доступ к управлению денежными средствами. Посредством Мобильного банка он сможет перевести деньги на свой или иной счет. Именно поэтому при потере телефона следует незамедлительно заблокировать сим-карту. Это можно сделать звонком оператору или в салоне связи.

! Звонок от лже-оператора или метод вишинга

Такой вид махинации с банковскими картами широко распространен от «лица» Сбербанка. Сперва на номер телефона держателя карты приходит смс с номеров похожих на 900 или 9000 о том, что для подтверждения перевода денег необходимо ввести код, иначе операция совершится самостоятельно (при этом, разумеется, владелец не проводил никаких действий с деньгами).

! Кража банковской карты

Самый примитивный вид мошенничества с чужой банковской картой – это ее кража. Воруют ее тогда, когда мошенникам известен пин-код. Поэтому настоятельно рекомендуется прикрывать от посторонних экран или клавиатуру банкомата при вводе пин-кода. Третьи лица могут подсмотреть комбинацию чисел, а затем незаметно для владельца завладеть его банковской карточкой и провести снятие наличности.

!Через Интернет

Перехват данных банковской карты при совершении крупных покупок в сомнительных интернет-магазинах, которые чаще имитируют известные магазины с незапятнанной репутацией. Мошенники запрашивают у доверчивых покупателей данные о кредитке: номер, срок действия, CVC/CVV код.

! Мошенники на «Авито»

Покупка товара с запросом о пин-коде. На такую уловку могут попасться как покупатели, так и продавцы. Мошенники под видом тех или

иных просят продиктовать им не только номер карты, но и пин-код, чтобы провести процесс оплаты якобы через свои ресурсы. Все это должно насторожить другую сторону и отказаться от предоставления лишних данных.

! Посредством Мобильного банка

Этот вирус позволяет мошенникам получать доступ не только в Мобильный банк потерпевшего, но и к его смс с одноразовыми паролями. Кроме того, троян может преграждать путь смс из банка о совершенных транзакциях на номер владельца карты, в результате чего последний долгое время не подозревает о финансовых махинациях.

! Скимминг

Скимминг – это разновидность мошенничества с банковскими картами, суть которого заключается в извлечении необходимой информации с магнитной ленты карт.

Для такого вида воровства безналичных средств применяют специальный аппарат – скиммер. Пин-код это устройство, конечно, не считывает, поэтому эта числовая комбинация вычисляется другими способами. Чаще всего для этого используют мини видеокамеры, встраиваемые в банкомат. Завладев всеми необходимыми данными карты, мошенники создают ее копию и могут снимать с ее электронного счета деньги.

! Шимминг

Шимминг – усовершенствованная форма скимминга. Усовершенствование заключается в использовании считывающего устройства – шима, которое совершенно незаметно.

! Фишинг

Фишинг – современный способ мошенничества с банковскими картами, осуществляемый через Интернет. Суть этого способа заключается в выманивании у людей их банковских данных: логинов, паролей, счетов, номеров и других необходимых сведений.

Чтобы обезопасить себя от подобной ситуации, специалисты рекомендуют придерживаться следующих мер:

- Не называть и не передавать никому пин-код.
- При введении пин-кода на клавиатуре банкомата необходимо загораживать клавиатуру и экран устройства. Стоящих сзади людей, стремящихся заглянуть за плечо, необходимо без стеснения попросить отодвинуться.
- При совершении покупок в Интернет-магазинах необходимо иметь надежную антивирусную систему на своем компьютере.
- Совершать покупки на непроверенных, не внушающих доверия сайтах не целесообразно.
- Не надо отвечать на все сомнительные смс, email-рассылки и неизвестные или скрытые номера, действующие якобы от имени банка.
- Ни в коем случае не сообщайте пин-код и ответ на секретный вопрос третьим лицам, в том числе и официальным сотрудникам банка.

Прокуратура Ленинского района г. Иркутска находится по адресу:

г. Иркутск, ул. Жукова, 7

Телефон: (395-2) 32-25-23