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.

Иркутская транспортная прокуратура
тел.: 8 (3952) 28-07-54
e-mail: vstp12@690.mailop.ru