Как не стать жертвой хищения денежных средств, совершаемых с использованием информационно-телекоммуникационных технологий

Повсеместно регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, у физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий.

Обмануть или взломать банковскую систему непросто, поэтому злоумышленники стараются любыми способами узнать необходимую информацию у самого держателя карты (счета).

Одним их самых распространенных способов хищения является получение доступа к конфиденциальным данным владельца банковской карты от него самого. Обычно преступники действуют с помощью почтовых рассылок, якобы от лица банка, сообщает о попытке взлома карты, снятии денежных средств, предлагают пройти по ссылке для возможного дальнейшего ее использования.

Другой способ мошенничества – звонок от имени технических и сервисных служб банка, которые под различными предлогами также пытаются получить конфиденциальную информацию по банковской карте.

Гражданам необходимо учитывать, что данные преступления являются трудно раскрываемыми ввиду применения злоумышленниками значительных мер конспирации, таких как оформление разовых абонентских номеров на лиц, не осведомленных об использовании их данных для совершения преступления, транзитных банковских счетов и счетов неперсонифицированных интернет-кошельков.

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

– выучите PIN-код наизусть или запишите на листок и храните отдельно от карточки, прикрывайте рукой клавиатуру банкомата или терминала в момент его ввода;

– никогда и никому не сообщайте код из СМС для подтверждения операции, которую клиент не совершал (сотрудники банка не вправе запрашивать данную информацию);

– не сообщайте конфиденциальные данные карты третьим лицам (номер банковской карты, PIN-код, секретный код безопасности CVV). Банки и операторы платежных систем никогда не присылают писем и не звонят клиентам с просьбой предоставить им данные о счете, PIN-код или иные персональные данные – вся информация у банка имеется;

– выбирайте банкоматы, расположенные внутри офисов, банков или в охраняемых точках оборудованных системами видеонаблюдения;

– не переходите по какой-либо ссылке в сообщениях, в которых вас просят;

– делая покупки в Интернет-магазинах, предварительно найдите реальный адрес продавца и его телефон, ознакомьтесь с отзывами;

– воздерживайтесь от предложений о легкой и высокой прибыли. Мошенники обычно настаивают на немедленном вложении денег, просят отправить деньги на оплату вымышленных налогов, сборов;

– не забывайте, что банки не рассылают сообщения о блокировке карт, а в телефонном разговоре не требуют конфиденциальные сведения и коды, связанные с картами клиентов. При необходимости свяжитесь с банком по официальным телефонам, которые также указаны на самой карте.

– немедленно блокируйте карту в случае утраты, кражи или захвате её банкоматом, а также при утере телефона с привязанным номером.

Старший помощник
межрайонного прокурора

младший советник юстиции М.А. Платова

СОГЛАСОВАНО:

Межрайонный прокурор

старший советник юстиции А.С. Новоселов