Приложение

Предупреждение хищений, совершенных с использованием современных информационно-коммуникационных технологий

Несмотря на постоянное информирование населения о наиболее распространённых способах неправомерного изъятия денежных средств граждан, число таких преступлений ежегодно увеличивается.

Необходимо знать, что подавляющее большинство преступлений указанной категории совершается с применением методов «социальной инженерии», то есть доступа к информации с помощью телекоммуникационных сетей для общения с потерпевшими (сотовой связи, ресурсов сети Интернет).

Технология основана на использовании слабостей человеческого фактора и является достаточно эффективной. Преступник может позвонить человеку, являющемуся пользователем банковской карты (под видом сотрудника службы поддержки или службы безопасности банка) и выяснить пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе или с банковским счетом, зачастую дезинформируя о его блокировке.

Распространенный характер носят хищения, связанные с другим способом обмана доверчивых граждан. Преступники, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации. К примеру, в связи с необходимостью освобождения их от уголовной ответственности. Нередко злоумышленники сами представляются сотрудниками органа правопорядка.

Дистанционные хищения совершаются посредством размещения на открытых сайтах в сети Интернет заведомо ложных предложений об услугах и продаже товаров за денежное вознаграждение, которое в дальнейшем перечисляется на банковский счет виновного лица. Преступники реализуют множество других способов и инструментов для завладения чужими деньгами: используют дубликаты сим-карт потерпевших, а также устройства-скиммеры, считывающие информацию, содержащуюся на магнитной полосе банковской карты для последующего изготовления ее дубликата. Рассылают в социальных сетях со взломанных страниц пользователей сообщения их знакомым с просьбами одолжить деньги, внедряют вредоносные программы в системы юридических лиц, похищают электронные ключи и учетные записи к нему в офисах организации и т.д.

Изменить эту ситуацию возможно в том случае, если граждане при общении с неизвестными лицами будут проявлять повышенную бдительность и более ответственнее подходить к сохранности своих сбережений.