Осторожно, мошенники!

Несмотря на постоянное информирование населения о наиболее распространённых способах неправомерного изъятия денежных средств граждан, преступления о хищениях, совершенных с использованием современных информационно-коммуникационных технологий, продолжают иметь место.

Большую их часть составляют кражи и мошенничества. Выявлять применяемые преступниками способы таких хищений и эффективно противостоять им намного сложнее, чем обычным преступлениям, изменить эту ситуацию можно в том случае, если граждане при общении с неизвестными лицами будут проявлять повышенную бдительность, более ответственно подходить к вопросу сохранности своих сбережений.

Необходимо знать, что большинство таких преступлений совершается с применением методов «социальной инженерии». Эта технология основана на использовании слабостей человеческого фактора.

Например, злоумышленник может позвонить человеку, являющемуся пользователем банковской карты (под видом сотрудника службы поддержки или службы безопасности банка), и выяснить пароль, сославшись на необходимость решения проблемы в компьютерной системе или с банковским счетом.

Распространенный характер носят хищения, связанные с убеждением граждан оформить кредиты, а полученные средства перевести на «безопасные счета». Преступники, представляясь сотрудниками банка, а также представителями правоохранительных органов, ложно информируют граждан о попытках хищения с их счетов денежных средств или оформления от их имени кредитов, для предотвращения которых требуется самостоятельное получение кредита и перевод денежных средств на «безопасный счет».

Дистанционные хищения также 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.

Денежные средства неправомерно списываются со счетов потерпевших, когда в руки преступников попадают их мобильные телефоны  
с установленными банковскими сервисами. То же самое касается и банковских карт: похитителями совершаются покупки путем оплаты товаров бесконтактным способом, при наличии пароля доступа – деньги снимаются в банкоматах.

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.

Активно применяют возможности «IP-телефонии». С применением различных компьютерных программ и интернет-ресурсов формируются любые номера абонентов, в том числе выдаваемые за номера правоохранительных органов и кредитно-финансовых организаций.

Вместе с тем, имеются способы мошенничества, когда инициатива передачи денежных средств мошенниками происходит по собственной инициативе граждан. Получают все большее распространение мошенничества прикрываемые привлечением денежных средств в инвестиционные проекты, в том числе криптовалюта, участие через брокера в операциях на фондовых рынках.

При должной внимательности можно распознать мошенников, так как практически все преступные схемы обладают характерными признаками:

- мошенники первыми выходят на контакт (поступает звонок,   
SMS-сообщение, электронное письмо и т.д.);

- они сообщают о возможной потере денежных средств, либо о выигрыше;

- запрашивают персональные данные (реквизиты банковских карт, коды-подтверждения) или просят установить что-либо по направляемым интернет-ссылкам для «защиты денежных средств»;

- действия мошенников всегда направлены на вызов сильных эмоций – напугать потерей денежных средств или обрадовать случайным выигрышем;

- всегда требуют принятия немедленных решений».

С.Д. Панафидин