О предупреждении хищений с использованием современных информационно-коммуникационных технологий

Развитие технологий в современном мире обуславливает их проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие различные противоправные цели, в том числе личное обогащение

Несмотря на постоянное информирование правоохранительными органами населения о наиболее распространённых способах неправомерного изъятия денежных средств граждан, положительного результата не достигнуто, число таких преступлений ежегодно увеличивается в геометрической прогрессии.

Выявлять применяемые преступниками способы таких хищений и эффективно противостоять им намного сложнее, чем обычным преступлениям, изменить эту ситуацию возможно в том случае, если граждане при общении с неизвестными лицами будут проявлять повышенную бдительность, более ответственнее подходить к сохранности своих сбережений.

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. Например, 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.

Денежные средства неправомерно списываются со счетов потерпевших, когда в руки преступников попадают их мобильные телефоныс установленными на них 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: 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.

Следует отметить, что число указанных противоправных деяний продолжает увеличиваться. Высокая степень общественной опасности таких преступлений подтверждается их спецификой - совершить их могут лица, обладающие специальными знаниями и использующие технические средства именно в криминальных целях, что приводит к нарушению не только права собственности, но и банковской тайны.

Необходимо быть крайне бдительными. Сотрудник банка не имеет право спрашивать пароль от карты и уж тем более, его нельзя никому сообщать. Чтобы не стать жертвой подобной аферы, достаточно повесить трубку и перезвонить в банковскую организацию по телефону, указанному на официальном сайте или на обороте карты. Уточните у оператора, действительно ли кто-то пытается снять деньги и сообщите номер телефона мошенников.

 Будьте внимательны! Пользуйтесь последними версиями браузеров и лицензионного антивирусного ПО. Следите за тем, что бы при входе на сайты было установлено защищенное соединение https.

О подобных фактах следует незамедлительно сообщать в правоохранительные органы, в первую очередь – в полицию. Такие сообщения тщательно проверяются в целях установления лиц, причастных к преступной схеме, и их привлечения к уголовной ответственности.

Заместитель прокурора района Э.О. Макашева