Как не стать жертвой мошенников

Развитие технологий в современном мире обуславливает их повсеместное проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие различные противоправные цели – личное обогащение, дискредитацию граждан и государственных органов, распространение нелегальной информации, идей терроризма и экстремизма.

В Российской Федерации отмечается ежегодный рост таких преступлений. Повсеместно регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий, ответственность за которые предусмотрена ст.ст. 158, 159, 159.3, 159.6 УК РФ.

Зачастую в совокупности с ними совершаются преступления в сфере компьютерной информации или так называемые киберпреступления, которые на практике нередко используются в качестве инструментария завладения чужим имуществом. В целях борьбы с компьютерной преступностью в УК РФ предусмотрена ответственность за ряд специальных составов, криминализирующих такие деяния, как: неправомерных доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).

Подавляющее большинство хищений рассматриваемой 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 по телефону и под видом сотрудника службы безопасности или службы поддержки банка, выведать пароль, сославшись на решение 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.

Дистанционные хищения совершаются посредством размещения на открытых сайтах 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 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.

Социальная инженерия используется также для распространения троянских коней. Злоумышленник направляет e-mail, sms-сообщение или сообщение в мессенджере, во вложении которого содержится, например, важное обновление антивируса или выгодное предложение о покупке со скидкой или фиктивном выигрыше с приложенной ссылкой при переходе по которой на устройство пользователя скачивается вредоносная программа. После чего преступник получает удаленное управление и возможность осуществления перечисления денежных средств со счета привязанной к абонентскому номеру банковской карты.

Необходимо отметить, что криминальные методы «удаленного» хищения денежных средств постоянно эволюционируют, при этом преступниками активно используются современные IT-технологии, которые зачастую просты в использовании и доступны неограниченному числу пользователей глобальной сети.