Хищения, совершаемые с использованием информационно-телекоммуникационных технологий

На сегодняшний день информационные технологии проникли во все сферы повседневной жизни каждого человека. Этим зачастую пользуются злоумышленники, преследующие противоправные цели, как правило связанные с хищением денежных средств.

В Российской Федерации отмечается рост количества таких преступлений, регистрируются преступления, связанные с хищением денежных средств граждан, находящихся на счетах в банках, с использованием современных информационно-коммуникационных технологий, ответственность за которые в зависимости от способа совершения преступления предусмотрена статьями 158, 159, 159.3, 159.6 УК РФ.

Большинство хищений в рассматриваемой сфере совершается путем введения граждан, имеющих открытые в кредитных организациях счета, в заблуждение с использованием телекоммуникационных сетей для общения с потерпевшими (сотовой связи, сети «Интернет»), практика показывает, что данный способ является весьма эффективным.

Например, злоумышленник может позвонить человеку, представившись работником службы поддержки или службы безопасности банка, путем обмана получить сведения о данных банковской карты, сославшись на необходимость решения той или иной проблемы.

Распространены хищения, связанные и с другими способами обмана граждан.

Так, преступники, представляясь родственниками либо знакомыми потерпевших, просят о перечислении денежных средств, в связи со сложившейся неблагоприятной ситуацией. Например, для разрешения каких-либо претензий со стороны правоохранительных органов.

Также, дистанционные хищения зачастую совершаются путем размещения на сайтах в сети «Интернет» заведомо ложных сведений об оказываемых услугах и купле-продаже товаров.

Денежные средства похищаются с банковских счетов граждан и когда в руки злоумышленников попадают мобильные телефоны с установленными приложениями кредитных организаций. Это же касается потерянных и украденных банковских пластиковых карт, большинство из которых в настоящее время имеют функцию бесконтактной оплаты, при совершении покупок на небольшие суммы (как правило до 1 000 рублей) с использованием данной функции введение PIN-кода не требуется.

Имеются случаи, когда по предложению преступников доверчивые граждане устанавливают на свои мобильные телефоны приложения, предоставляющие злоумышленникам удаленный доступ к телефону, после чего получают возможность перечислить денежные средства со счета привязанной к номеру телефона банковской карты.

Часто люди поддаются на обещания легкой прибыли, содержащиеся на различных Интернет-ресурсах. После регистрации на сайте и введения личных

данных в контакт с гражданином вступает злоумышленник, который обещаниями легкого и значительного заработка без приложения к этому каких-либо усилий со стороны гражданина, добивается перевода последним денежных средств. Для усыпления бдительности гражданина на сайте размещается информация о растущей прибыли, в то же время при желании получить свои деньги гражданин сталкивается с препятствиями в виде неиссякаемых предложений дополнительно оплатить страховку, внести залог и т.п.

Как способ совершения преступления используется «фишинг». Злоумышленник направляет потерпевшему электронное письмо, СМС-сообщение либо сообщение в мессенджере, имитирующее официальное обращения со стороны банка и требующее проверки информации либо совершения тех или иных действий. Сообщение содержит ссылку на поддельный Интернет-сайт, имитирующий настоящий, и содержащий форму, требующую ввести необходимую для злоумышленника информацию – данные банковской карты, ПИН-код, паспортные данные и т.п.

Такие способы совершения преступлений не теряют свою эффективность, так как цифровизация многих правоотношений затрагивает уязвимые для противоправных действий слои населения, например, пожилых людей, которые испытывают сложности при работе с современной техникой, а также страдают чрезмерной доверчивостью.

Преступники используют и иные способы хищения денежных средств: изготавливают дубликаты SIM-карт потерпевших, рассылают в социальных сетях со взломанных страниц пользователей сообщения их знакомым с просьбами занять деньги и т.д. При этом методы дистанционного хищения денег постоянно эволюционируют, преступники активно используют современные технологии, которые в отдельных случаях просты в использовании и доступны неограниченному числу пользователей.

Для того, чтобы замести следы преступления злоумышленники меняют телефоны, оформляют SIM-карты и открывают счета в банках на подставных лиц, в том числе иностранных граждан, используют электронные кошельки, привлекают лиц, не осведомленных о противоправности их действий, применяют другие способы, делающие зачастую раскрытие таких преступлений в существующих условиях невозможным.

В случае поступления предложений предоставить данные своей банковской карты, установить приложение либо указать иную информацию, к ним необходимо относиться критически, информацию перепроверять путем самостоятельных звонков на горячую линию кредитной организации. При поступлении звонков либо сообщений от «родственников» прежде чем переводить деньги необходимо самостоятельно созвониться с ними, выяснив их местонахождение и иные обстоятельства. При утере банковских карт следует незамедлительно позвонить по горячей линии в банк и потребовать заблокировать утерянную карту.

О предполагаемых фактах хищений незамедлительно сообщать в органы внутренних дел.