**Томская транспортная прокуратура разъясняет о противодействии в сфере информационно-телекоммуникационных технологий**

С учетом развития информационно-телекоммуникационных технологий, развивается и преступность в указанном направлении, в связи с чем, остро стоит вопрос противодействия обману и хищениям, совершенным с использованием современных информационно-телекоммуникационных технологий.

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

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. Так называемый фишинг - техника «социальной инженерии», направленная на получение конфиденциальной информации.

Обычно злоумышленник посылает потерпевшему e-mail, подделанный под официальное письмо – от банка или платежной системы – требующее «проверки» определенной информации, или совершения определенных действий.

Это письмо как правило содержит ссылку на фальшивую веб- страницу, имитирующую официальную, с корпоративным логотипом и содержимым, и содержащую форму, требующую ввести необходимую для преступников информацию – от домашнего адреса до пин-кода банковской карты.

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 ним в офисах организаций и т.д. Активно применяются возможности «IP-телефонии».

С использованием различных компьютерных программ и интернет-ресурсов формируются любые номера абонентов, в том числе выдаваемые за номера правоохранительных органов и кредитно-финансовых организаций.

Кроме того, существуют способы мошенничества, когда инициатива передачи денежных средств мошенникам 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.

Перед тем как переводить свои денежные средства необходимо убедиться в наличии у организации лицензии на привлечение денежных средств граждан, лицензии на ведение брокерской деятельности - реестр брокеров размещен на официальном сайте Банка России.

Кроме того, не следует переводить и передавать денежные средства незнакомым лицам, действующим под различными предлогами, в том числе по поручению или от имени родственников или знакомых.