Прокуратура Российской Федерации

Прокуратура Тульской области

ИНФОРМАЦИЯ

«О наиболее распространенных способах хищений, совершаемых с использованием информационно-коммуникационных технологий, и порядке обращения в правоохранительные органы за защитой прав»

Проблема защиты граждан от хищений с использованием информационно-коммуникационных технологий продолжает оставаться крайне актуальной. Анализ данных уголовно-правовой статистики свидетельствует о росте числа таких преступных деяний. К наиболее типичным способам их совершения можно отнести следующие.

Злоумышленники звонят гражданам, представляясь сотрудниками банков, называя их по имени, отчеству, просят сообщить данные банковских карт (номер, CVC (CVV), PIN-коды и т.п.) для предотвращения якобы несанкционированного списания денежных средств либо оформления кредита. Используя персональные данные, получают удаленный доступ к личному кабинету клиента банка, осуществляют перевод денежных средств без ведома собственника. При этом, как правило, преступники используют программы подмены телефонных номеров, в связи с чем номер входящего звонка определяется у клиента как номер банка.

Зачастую введенные в заблуждение граждане сами переводят денежные средства на счета, указанные мошенниками. Распространены хищения с использованием преступниками сервиса «Avito». Вводя гражданина в заблуждение относительно своего намерения приобрести или продать товар, в ходе телефонных разговоров злоумышленники узнают интересующие реквизиты банковской карты потерпевшего, при помощи которых впоследствии списывают денежные средства со счета независимо от воли законного владельца.

В ряде случаев предлагается перейти по ссылкам, на которые указывает лжепродавец, для последующего перевода денежных средств, после чего такое лицо не предоставляет оплаченный товар и не выходит на связь. Кроме этого, преступники, используя базы данных компаний мобильной связи, массово рассылают SMS-сообщения следующего содержания: «Ваша карта заблокирована. Для разблокировки необходимо позвонить по номеру...».

Большинство граждан, вместо того, чтобы сразу обратиться в ближайший офис своего банка для проверки поступившей информации либо осуществить звонок в службу клиентской поддержки,

перезванивают по указанному в SMS-сообщении номеру, в ходе разговора передают злоумышленникам информацию о банковских реквизитах, в том числе о PIN-коде, после чего осуществляется незаконное списание денежных средств. Зачастую граждане сами переводят денежные средства на указанные преступниками «защищенные» счета якобы для их сохранения. Фактически денежные средства выбывают из законного владения, и собственник не имеет к ним доступа.

Хищения денежных средств у граждан совершаются также путем направления SMS-сообщений о выигрыше, для получения которого необходимо перевести денежные средства на указанный абонентский номер. Распространены факты, когда преступники представляются родственниками либо знакомыми потерпевших, рассказывают, что попали в беду (стали виновником дорожно-транспортного происшествия, задержаны сотрудниками полиции, срочно требуются деньги на операцию и тому подобное) и просят срочно предоставить им денежные средства. Более того, злоумышленники взламывают электронную почту, аккаунты в соцсетях, после чего от имени пользователя рассылают гражданам, сведения о которых имеются в контактах данного лица, просьбы о займе денежных средств, в результате деньги поступают на счет мошенника.

Неединичными продолжают оставаться факты мошенничества посредством сбыта через интернет-магазины «чудо-приборов», техники, препаратов и лекарств, товаров и услуг по якобы льготным расценкам, а фактически по завышенной цене. Иногда потерпевшие получают товары и услуги ниже заявленного качества или не получают их вовсе. Имели место факты перевода крупных денежных сумм мошенникам в счет оказания экстрасенсорных услуг. Потерпевшие, будучи введенными в заблуждение, переводили за «снятие порчи», «предсказание судьбы», «очистку кармы» злоумышленникам денежные средства.

Выявлены случаи навязывания услуг якобы по защите прав лиц, ранее пострадавших от преступных посягательств либо в результате действий недобросовестных поставщиков товаров и услуг. Представляясь сотрудниками государственных органов либо организаций, осуществляющих помощь гражданам, которым причинен ущерб, под вымышленными предлогами (оплата труда адвоката, составление искового заявления, комиссия за перевод денег в счет компенсации ущерба, несуществующий налог) требуют передачи денежных средств, фактически не имея намерений выполнять взятые обязательства.

Для минимизации возможных потерь и защиты владельцев банковских карт необходима простая бдительность и осторожность граждан. Категорически нельзя сообщать посторонним лицам данные карты, персональные данные и коды, присланные в СМС; предоставлять таким лицам доступ к банковской карте через онлайн-банкинг. В любых подозрительных ситуациях нужно звонить в банк, выдавший карту, по номеру, указанному на ее оборотной стороне, либо самим перезванивать лицам, от имени которых представились мошенники. Следует не поддаваться желанию получить сомнительный выигрыш либо компенсацию и не переводить для этого денежные средства, а также оплачивать товар только после его получения, не пользоваться сомнительными услугами.

В случаях, если гражданин пострадал от мошеннических действий с банковскими картами, необходимо незамедлительно обратиться в банк, сообщить, что списание денежных средств произошло против воли собственника, заблокировать карту, получить выписку о движении денежных средств по счету (по возможности), подать заявление в правоохранительные органы. В любом случае, если совершаются или совершены мошеннические действия, необходимо обратиться лично с заявлением о преступлении в любой территориальный орган МВД России (подразделение полиции) либо по телефону.