Чтобы не стать жертвой преступлений, совершаемых в сфере информационно-коммуникационных технологий или с использованием компьютерной информации

Случаи совершения преступлений, связанных с посягательствами на безопасность в сфере использования информационно-коммуникационных технологий, получают все большее распространение.

Одно из наиболее часто встречающихся подобных преступлений – хищение денежных средств со счетов граждан с использованием реквизитов банковских карт. Преступники, чаще всего, получают такие реквизиты в телефонном разговоре.

Чтобы не стать жертвой злоумышленников необходимо помнить следующее. Сотрудники банка по телефону никогда не запрашивают реквизиты карты – ее номер, срок действия, трехзначный код на обороте. Если сотрудник банка по телефону просит совершить какие-либо операции с картой – это признак мошенничества. Никому не сообщайте код подтверждения операции из СМС. При сомнительных звонках следует прервать телефонный разговор и перезвонить в банк, клиентом которого Вы являетесь.

Хищение денежных средств может быть совершено также при совершении онлайн-покупок. При совершении онлайн-продажи товара для получения денег от покупателя достаточно сообщить только номер банковской карты. Если вас просят указать другие реквизиты (например, CVV-код) – это признак мошенничества.

Имеют место случаи мошенничества с использованием социальных сетей. Например, преступник, обнаружив сохраненный логин и пароль от страницы гражданина в социальной сети, может без разрешения зайти на эту страницу, поменять логин, пароль и от имени гражданина осуществить рассылку друзьям (знакомым) последнего писем с просьбой об одолжении денежных средств. Лицу, получившему такое письмо, следует связаться с гражданином, от имени которого направлена просьба об одолжении денежных средств, и удостовериться в подлинности письма.

Предупреждение, выявление, раскрытие и расследование преступлений, совершенных с использованием информационно-коммуникационных технологий (ИКТ).

Активное развитие современных ИКТ порождает новые угрозы государственной и общественной безопасности. С ростом количества телекоммуникационных устройств и пользователей информационных сетей увеличивается число потенциальных жертв, а также возрастают возможности эксплуатации сети интернет для совершения противоправных деяний. В этой связи проблема защиты граждан от хищений с использованием

информационно-коммуникационных технологий, а также восстановления их имущественных прав является крайне актуальной.

Особая сложность раскрытия и расследования подобных преступлений обусловлена анонимностью злоумышленников и отсутствием непосредственного контакта с потерпевшим, охватом широкой аудитории, простотой доступа к информации, а также организованным и трансграничным характером посягательств.

Существенное влияние на увеличение количества преступлений, совершаемых с использованием информационно-коммуникационных технологий, оказывает активное развитие новых форм платных услуг и сервисов, а равно применение в расчетах цифровых средств платежей.

Наиболее типичные способы совершения таких преступлений:

Использование так называемых «фишинговых» сайтов (от англ. «fishing» - рыбная ловля). Злоумышленники звонят гражданам и сообщают о компенсационных выплатах, выигрышах в лотерею, перерасчете пенсий и пособий и т.д. Потерпевший переходит на интернет-страницу по ссылке, указанной преступниками, где ему предлагают ввести свои личные данные, реквизиты банковских карт либо иные конфиденциальные сведения, с помощью которых потом мошенники похищают денежные средства.

Использование сервисов «Avito», «Юла» и т.п. Введя гражданина в заблуждение относительно своего намерения приобрести или продать товар, злоумышленники в ходе телефонных разговоров узнают реквизиты банковской карты потерпевшего, при помощи которых впоследствии списывают денежные средства со счета законного владельца. В ряде случаев потерпевшему предлагается перейти по ссылкам, которые указывает фиктивный продавец или покупатель, на «фишинговые» сайты для последующего перевода (получения) денежных средств, после чего мошенник, списав деньги со счета потерпевшего, уже не выходит на связь.

Незаконный доступ к компьютерной информации. Злоумышленники, осуществив несанкционированный доступ к странице пользователя социальной сети (в том числе путем ее взлома), вводят других пользователей (в основном, знакомых с ним) в заблуждение, рассылая им от имени владельца страницы сообщения с просьбой одолжить либо пожертвовать деньги, как правило, для экстренных нужд (оплата дорогостоящего лечения, покупка необходимой вещи и т.п.).

«Социальная инженерия», то есть моделирование ситуаций, в которых потерпевший становится «марионеткой» в руках мошенников. Преступники, представляясь сотрудниками банков либо правоохранительных органов, просят потерпевшего сообщить данные банковских карт (номер, CVC (CVV), PIN-коды и т. п.) якобы для предотвращения несанкционированного списания денежных средств либо оформления кредита. Используя

персональные данные, злоумышленники получают удаленный доступ к личному кабинету клиента банка и осуществляют перевод денежных средств без его ведома. При этом, как правило, используются программы подмены телефонных номеров, в связи с чем номер телефона, с которого осуществляются входящие звонки, определяется у клиента как номер банка либо правоохранительного органа. Иногда потерпевшие, поддавшись психологическому воздействию мошенников, искренне верят, что участвуют в поимке членов организованной преступной группы, и в течении нескольких дней безропотно выполняют все указания злоумышленников: оформляют кредиты в банках, продают свои автомобили и даже квартиры, с последующим переводом денежных средств на банковские карты (счета) третьих лиц. Необходимо отметить, что порядок осуществления соединений между абонентами (операторами сотовой связи) регулируется Федеральным законом от 07.07.2003 № 126-ФЗ «О связи». За пропуск операторами сотовой связи теневого трафика и оказание услуг по организации соединений между абонентами, использующими подменные номера, ч. 3 ст. 14.1, ст. 13.2.1 КоАП РФ предусмотрена административная ответственность и наказание в виде штрафа в размере до миллиона рублей.

В случаях, если гражданин пострадал от мошеннических действий, связанных с незаконными банковскими операциями, ему 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), а также обратиться в любой территориальный орган МВД России (подразделение полиции) лично либо по телефону.