Противодействие преступности 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.

Выявлять применяемые преступниками способы таких хищений и эффективно противостоять им намного сложнее, чем обычным преступлениям, изменить эту ситуацию можно в том случае, если граждане при общении с неизвестными лицами будут проявлять повышенную бдительность, более ответственно подходить к вопросу сохранности своих сбережений.

Необходимо знать, что большинство таких преступлений совершается с применением методов «социальной инженерии». Эта технология основана на использовании слабостей человеческого фактора.

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

Распространенный характер носят хищения, связанные с убеждением граждан оформить кредиты, а полученные средства перевести на «безопасные счета». 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 — тоже 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.

При должной внимательности граждане могут распознать мошенников, так как практически все преступные схемы обладают характерными признаками:

— мошенники первыми выходят на контакт (поступает звонок, SMS-сообщение, электронное письмо и т.д.);

— они сообщают о возможной потере денежных средств, либо о выигрыше;

— запрашивают персональные данные (реквизиты банковских карт, коды-подтверждения) или просят установить что-либо по направляемым интернет-ссылкам для «защиты денежных средств»;

— действия мошенников всегда направлены на вызов сильных эмоций – напугать потерей денежных средств или обрадовать случайным выигрышем;

— всегда требуют принятия немедленных решений.

Важно помнить, что нельзя никогда и никому сообщать трёхзначный код на обратной стороне банковской карты (CVV), а также личные сведения, данные банковских карт и счетов, поступившие в СМС пароли, которые могут быть использованы злоумышленниками для неправомерных действий.

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

Помимо того, на территории России участились случая телефонных мошенников с Украины, представляющимися «Российскими спецсслужбами».

В прошлом году по России прокатилась волна поджогов военкоматов, полицейских автомобилей, банкоматов и прочего.

Среди лиц, совершивших преступления были, в том числе женщины средних лет и пенсионеры, прежде не фигурировавшие в делах об экстремизме или терроризме.

В последствии установлено, что все они пострадали от действий телефонных мошенников: преступники убедили их, что поджоги военкоматов, и прочего — это задание российских спецслужб.

Так, представляясь сотрудниками ФСБ России, а также службы безопасности банков, мошенники, используя психологические приемы, предлагают гражданам принять участие в оперативно-разыскных мероприятиях по поимке преступников.

В частности, мошенники просят оказать помощь в изобличении с поличным преступников, для чего предлагают оформить кредит, либо продать имущество и перечислить средства на «защищенные банковские счета».

В дальнейшем, получив денежные переводы, «телефонные мошенники» могут также заявить, что в отношении гражданина, который перечислил деньги может быть возбуждено уголовное дело за финансирование терроризма и уже начинают открыто склонять к совершению поджогов объектов и автомобилей в местах массового скопления людей, что уже формирует состав преступления, предусмотренного статьей 205 УК России «Террористический акт»

Статья 205 Уголовного кодекса Российской Федерации предусматривает уголовную ответственность за совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, в целях воздействия на принятие решения органами власти или международными организациями, а также угроза совершения указанных действий в тех же целях. Наказание за совершение указанных действий предусматривает от 10 лет лишения свободы и до пожизненного лишения свободы.