О мошенничестве с использованием сети Интернет и сотовой связи

Активное развитие информационных технологий, постоянное увеличение числа граждан ежедневно пользующегося возможностями сети Интернет и сотовой связью, закономерно приводит к ежегодному росту количества преступлений в рассматриваемых сферах. Наиболее часто встречающимся составом преступлений с использованием телефонной связи, сети Интернет является мошенничество. Жертвой телефонных и интернет мошенников может стать любой человек.

Основными видами «телефонных» мошенничеств являются:

- звонки от имени сотрудников правоохранительных органов о том, что родственник попал в ДТП, в полицию, в больницу и т.п., в связи с чем, для освобождения от уголовной ответственности, требуют передать определенную сумму денег;

- звонки о желании приобрести какое-либо имущество, размещенное на различных Интернет-сайтах гражданами в объявлениях о продаже.

В таких случаях мошенник звонит по объявлению и просит продиктовать номер банковской карты для перечисления аванса за товар, а потом просит сообщить различные коды доступа, с целью получения доступа к банковскому счету жертвы;

- звонки от имени сотрудников банков о хакерской атаке на кредитное учреждение, о блокировке банковской карты, задолженности по кредиту и т.п. В ходе общения мошенники просят сообщить различные коды доступа, либо совершить какие-либо операции, в результате злоумышленники получают доступ к банковскому счету жертвы;

- sms-сообщения либо звонки о каком-либо выигрыше (автомобиля, телефона и т.п.), для получения которого необходимо перечислить денежные средства.

Основными способами мошенничества в сети Интернет являются:

- размещение мошенниками на сайтах бесплатных объявлений («Авито», «АвтоРУ» и др.) предложений о намерении покупки или продажи какого-либо имущество, в последующем, в ходе общения злоумышленник предлагает осуществить предоплату или аванс. В результате, перечислив денежные средства, жертва не получает ни услугу, ни товар;

- неправомерный доступ к конфиденциальным данным пользователей («фишинг»)

– к логинам и паролям банковских карт, интернет-кошельков, сервисам интернет-банкинга. Данный вид мошенничества осуществляется, как правило, с использованием вредоносного программного обеспечения, в том числе путем заражения компьютеров, мобильных устройств «вирусами» через рассылку электронных писем, рекламу, незнакомые интернет-сайты;

- мошеннические интернет-магазины, после совершения покупки в которых клиент в лучшем случае получит некачественную услугу или товар, а в худшем останется ни с чем;

- объявления в социальных сетях о помощи в денежном эквиваленте, на лечение ребенка, родственника или для преодоления иных сложных

жизненных ситуаций. Такие объявления могут быть вовсе фиктивными, либо мошенники могут использовать реальные объявления, в том числе с сайтов известных благотворительных организаций, с изменёнными банковскими реквизитами;

- разнообразные схемы мошенничества с удаленной работой, когда злоумышленники представляются в виде работодателей и предлагают быстрый заработок (сбор ручек, перепечатывание текста, платные опросы). Однако обычно для начала работы необходимо приобрести так называемый «стартовый набор», зарегистрироваться на платном интернет ресурсе, либо произвести иные платежи. В итоге либо материалы для работы не приходят вовсе, либо жертвы получают бесполезные товары, инструкции, схемы «пирамид» и т.п.

Приведенные способы телефонного и сетевого мошенничества не являются исчерпывающими, существует множество вариаций приведенных схем, а также регулярно мошенниками разрабатываются новые механизмы хищения денежных средств. Но во всех случаях мошенники имеют цель – заставить человека передать свои деньги «добровольно». В зависимости от способа, размера причиненного ущерба и характеристики субъекта преступной деятельности, действия мошенников квалифицируются по статьям 159 (Мошенничество) либо 159.6 (Мошенничество в сфере компьютерной информации) Уголовного кодекса Российской Федерации. Несмотря на имеющуюся практику расследования и рассмотрения уголовных дел указанной категории, необходимо проявлять осторожность в общении по телефону с незнакомыми людьми и при совершении финансовых операций в сети Интернет, помнить о необходимость проверки сведений.