Способы совершения преступлений с использованием информационно-телекоммуникационных технологий

В современном мире интернет проник во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие различные противоправные цели - личное обогащение, дискредитацию граждан и государственных органов, распространение нелегальной информации, идей терроризма и экстремизма.

Подавляющее большинство киберпреступлений совершается с применением методов «социальной инженерии», то есть доступа к информации с помощью сети Интернет для общения с потенциальными жертвами обмана. Технология основана на использовании психологических слабостей человека и является достаточно эффективной. Частный пример - преступник, под видом сотрудника службы поддержки банка, звонит человеку, являющемуся пользователем банковской карты и узнает пароль, сославшись на необходимость решения небольшой проблемы в компьютерной системе или с банковским счетом, зачастую дезинформируя о его блокировке.

Распространенный характер носят хищения, связанные с другим способом обмана доверчивых граждан. Преступники, представляясь близкими родственниками (знакомыми) потерпевших, просят о передаче или перечислении электронным платежом определенной суммы денежных средств для разрешения сложившейся в их жизни неблагоприятной ситуации. К примеру, в связи с необходимостью освобождения их от уголовной ответственности. Нередко злоумышленники сами представляются сотрудниками органа правопорядка.

Одной из распространенных методов «социальной инженерии» является так называемый «фишинг». Данный метод направлен на получение конфиденциальной информации. Обычно преступник посылает потерпевшему e-mail (письмо на электронную почту), 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, которая является полной копией официального интернет-источника. На фальшивой странице пользователю требуется ввести необходимую для преступников информацию – от домашнего адреса до пин-кода банковской карты.

Также злоумышленники зачастую используют и активно распространяют вредоносные программы, такие как «Троянский конь». Злоумышленник направляет e-mail, sms-сообщение или сообщение в мессенджере, во вложении которого содержится, например, важное обновление антивируса. Это может быть выгодное предложение о покупке

со скидкой или сообщение о фиктивном выигрыше с приложенной ссылкой, при переходе по которой на устройство пользователя скачивается вредоносная программа. После чего преступник получает удаленное управление и возможность осуществления перечисления денежных средств со счета привязанной к абонентскому номеру банковской карты.

Необходимо отметить, что криминальные методы «удаленного» хищения денежных средств постоянно эволюционируют, при этом преступниками активно используются современные IT-технологии, которые зачастую просты в использовании и доступны неограниченному числу пользователей глобальной сети.

В целях пресечения указанных видов преступлений призываем всех быть предельно внимательными при осуществлении банковских операций с использованием сети «Интернет» и мобильных телефонов. Не поддавайтесь на уловки мошенников и всегда перепроверяйте полученную информацию.

Если вы или ваши близкие стали жертвами мошенников, незамедлительно обращайтесь в органы внутренних дел.