Профилактика преступлений, совершенных 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.

К наиболее распространенным видам дистанционных мошенничеств относятся:

- **«фишинг»** – вид дистанционного мошенничества, при совершении которого злоумышленники (в ходе телефонного разговора, посредством направления электронного письма или смс-сообщения) получают личные конфиденциальные данные о банковской карте, номере счета, логины и пароли для входа в интернет-банк, а также пароли безопасности, позволяющие произвести списание находящихся на банковской карте денежных средств. Жертвами указанного вида мошенничества зачастую становятся незащищенные, малообразованные, доверчивые слои населения. Представляясь зачастую сотрудниками кредитных организаций, преступники вводят в заблуждение граждан относительно совершаемых несанкционированных списаний денежных средств, осуществляемых покупках и т.п., после чего просят назвать конфиденциальные сведения с целью пресечения возможного совершения преступления. Граждане, доверяя полученной информации, желая обезопасить свои денежные средства от преступных посягательств, сообщают запрашиваемую информацию, в результате чего злоумышленники похищают принадлежащие им денежные средства.

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.

- **«фарминг»** — процедура скрытого направления на ложный IP-адрес, то есть направление пользователя на фиктивный веб-сайт, чаще всего используемый для приобретения товаров и услуг (ozon.ru, avito.ru, aliexpress.ru, joom, biglion, купинатор, кассир.ру, билетер, сайты по продаже билетов на ж/д и авиатранспорт и др.);

- **«двойная транзакция»** (при оплате товаров и услуг продавец сообщает об ошибке, предлагает повторить операцию, а в дальнейшем денежные средства списываются дважды по каждой из проведенных операций)

-«траппинг» (манипуляции с картридером банкоматов, позволяющие либо не возвращать карту владельцу, либо списывать все данные карты для дальнейшего их использования).

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 Кирово-Чепецкая городская прокуратура призывает 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.

Старший помощник Кирово-Чепецкого
городского прокурора

младший советник юстиции Н.С. Кокорева