Правила безопасности в сфере противодействия преступлениям, совершенным с использованием информационно-телекоммуникационных технологий

Мошенниками разработано множество схем хищения денежных средств путем обмана или злоупотребления доверием:

– звонки с сообщением о мошеннических действиях с личным кабинетом на сайте Госуслуг;

– сообщение о подозрительных операциях с банковскими счетами, где в ходе разговора жертва переводит денежные средства на несуществующий «безопасный счет»;

– сообщение о подозрительных операциях с банковскими счетами, где для предотвращения хищения денежных средств необходимо установить специальную программу на мобильный телефон, а также зайти в приложение банка, после чего мошенник получает удаленный доступ к приложению банка, оформляет кредит и выводит денежные средства со счета жертвы;

– звонки «родственник в беде» - сообщение об участии родственника в дорожно-транспортном происшествии и его виновности в нем, о необходимости передачи денежных средств для оказания помощи пострадавшим и избежания привлечения родственника к уголовной ответственности;

– размещение в сети Интернет информации с предложением дополнительного «легкого» заработка путем ставок на бирже, в результате чего жертвы перечисляют свои личные сбережения на специальный счет, однако обратно получить их не могут, все денежные средства «уходят» на счета мошенникам.

Несмотря на многочисленные предупреждения правоохранительных органов, количество зарегистрированных сообщений о хищении денежных средств с использованием мобильной связи и сети Интернет растет, люди продолжают доверять незнакомцам по телефону.

Еще одна схема мошенников - извещение об истечении срока действия договора об оказании услуг мобильной связи.

Злоумышленник звонит жертве представляясь «оператором сотовой связи», сообщает о необходимости продления договора, для чего необходимо сообщить код из смс сообщения.

Далее жертве приходит уведомление о совершении входа в личный кабинет на сайте Госуслуг, где указан телефон службы поддержки. Жертва обращается в «службу поддержки», где ей сообщают о том, что с использованием ее персональных данных поданы заявки на оформление кредитов, в целях исключения возможности воспользоваться данным кредитом мошенники, уверяют жертву о необходимости оформления аналогичного кредита и перевода его на номер карты, который они укажут. Введенные в заблуждение граждане самостоятельно оформляют кредит, а

затем переводят полученные денежные средства на счет, который был указан мошенником.

Чаще всего подобные телефонные разговоры осуществляются посредством интернет мессенджеров (WhatsApp, Telegram). Сотрудники каких-либо организаций не осуществляют звонки через указанные мессенджеры.

Если Вам звонит «сотрудник банка» и сообщает о списаниях денежных средств с Вашего счета, о взломе Вашего личного кабинета или о попытке оформления кредита, «сотрудник оператора сотовой связи» о необходимости продления договора, «сотрудник правоохранительного органа» с сообщением о мошеннических действиях с вашими банковскими счетами - незамедлительно кладите трубку, независимо с какого номера телефона поступил звонок.

Для проверки информации перезвоните в банк, оператору сотовой связи либо в правоохранительный орган самостоятельно. Не производите никаких действий с банковской картой по указанию третьих лиц.

Так как за совершение данных незаконных действий предусмотрена уголовная ответственность, по статье 159 УК РФ, в случае если вы стали жертвой мошенников, обращайтесь с заявлением в органы полиции по месту совершения преступления.