

Информация
об основных схемах мошеннических действий, используемых
преступниками на территории автономного округа
в январе 2024 года

Перечень и основные характеристики дистанционных хищений:

1. Звонок сотрудника банка либо правоохранительных органов, рекомендующего под предлогом пресечения несанкционированного оформления кредита, хищения денежных средств с банковских счетов гражданина, оформить встречный кредит (зеркальная заявка) и направить средства на указанный мошенником счет.

2. Под предлогом заработка путем инвестиционных вложений предлагается перевести денежные средства с личных счетов на указанный мошенником счет.

3. Внесение предоплаты при совершении сделки по приобретению товаров (услуг) на сайте «Авито», в социальной сети «ВКонтакте», в группах мессенджеров «WhatsApp», «Viber», «Telegram».

4. Заем денежных средств «родственнику, знакомому» посредством отправления сообщений или осуществления звонков с известных потерпевшему номеров в мессенджерах «WhatsApp», «Viber», «Telegram».

При этом преступниками активнее стали использоваться вновь созданные схемы мошеннических действий:

1. Когда участниками преступления используется механизм поэтапного обмана потерпевшего, где на первом этапе «работник» сотового оператора под предлогом необходимости продления срока договора предоставления услуг мобильной связи предлагает гражданину сообщить ему смс-коды доступа к личному кабинету на сайте «Госуслуги», после чего уже «сотрудники» сайта «Госуслуги» и Центрального банка Российской Федерации под предлогом пресечения противоправных действий и сохранения денежных средств потерпевшего от несанкционированного перевода либо хищения убеждают его перевести личные сбережения либо кредитные средства на «безопасный банковский счет»;

2. Когда гражданину от лица руководителя сообщается о рекомендованном (обязательном) выполнении предложений сотрудников правоохранительных органов или работников банковских структур по перечислению личных сбережений либо оформлению встречной (зеркальной) заявки на кредит и последующего перечисления кредитных средств, якобы направляемых на пресечение несанкционированного

оформления кредита, попытки хищения денежных средств с банковских счетов потерпевшего»;

3. Когда в мошеннических схемах злоумышленники, используя доверчивость несовершеннолетних, их заинтересованность в получении легких доходов, желание помочь (защитить) родителей либо близких им людей от преступников, получив реквизиты банковских карт, совершают хищение личных сбережений, либо кредитных средств.

Для оказания большего давления на потерпевших зачастую перечисленные схемы дополняются информацией, что средства с их счетов несанкционированно переводятся на поддержку вооруженных сил Украины, в связи с чем, чтобы избежать уголовной ответственности за финансирование террористических организаций, требуется незамедлительное выполнение рекомендуемых действий.

В официальном телеграмм-канале мессенджера «Telegram» «Вестник киберполиции России» Управления по организации борьбы с противоправным использованием информационно-коммуникационных технологий Министерства внутренних дел Российской Федерации размещены информационные материалы по профилактике дистанционных хищений, содержащие сведения о схемах мошеннических действий, применяемых преступниками на территории Российской Федерации, здесь же можно оперативно получать информацию о новых схемах мошенничества (ссылка: https://t.me/cyberpolice_rus/1072).