Информация
о появлении новых и наиболее распространенных способах совершения преступлений с использованием информационно-телекоммуникационных технологий

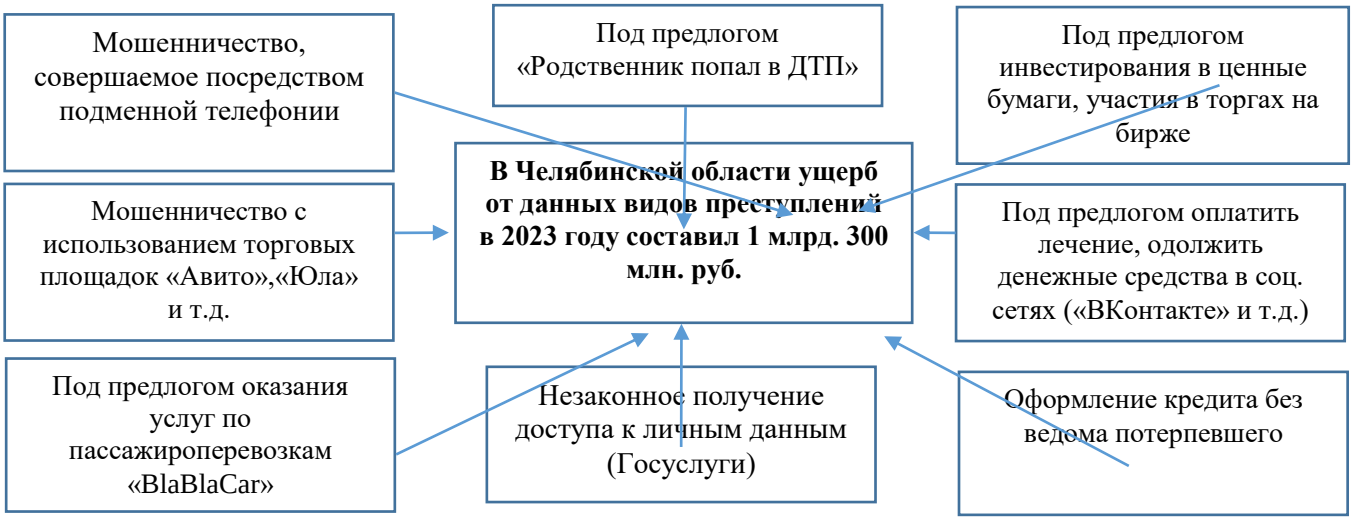
ГУ МВД России по Челябинской области информирует о появлении новых способах совершения дистанционных мошенничеств:

1. Функционирование Интернет-сайтов, имитирующих ресурсы государственных ведомств и справочных систем. Мошенники размещают шаблоны документов, которые ищут в сети «Интернет» бухгалтеры, секретари, сотрудники, занимающиеся налоговой или финансовой деятельностью. Шаблоны документов при этом заражены вирусами. Когда сотрудник загружает документ, на его компьютере запускается программа удаленного доступа. С ее помощью мошенники меняют в договорах компаний банковские реквизиты, чтобы впоследствии получить на свои счета денежные средства, предназначенные подрядчикам и заказчикам.

2. Предложения об установке на телефон (смартфон) программного обеспечения. Мошенники, представляясь сотрудниками банка, предлагают установить так называемое «официальное сертифицированное приложение» финансовой организации для проверки устройства и поиска уязвимостей. Далее злоумышленники отправляют потенциальным жертвам ссылку на фишинговый сайт с инструкцией по установке приложения. После установки программного обеспечения мошенники получают удаленный доступ к смартфону и выводят денежные средства из онлайн-банка клиента.

3. Сообщения от якобы Федеральной службы судебных приставов. Мошенники направляют гражданам электронные письма и сообщения об имеющейся задолженности, информируя (или угрожая) внести должника в некий «федеральный реестр недобросовестных плательщиков» и заблокировать его банковские счета (банковские карты). Чтобы этого избежать, предлагают пройти по поступившей ссылке для погашения имеющейся задолженности. После перехода по ссылке, денежные средства перечисляются на счета мошенников.

Кроме того, в настоящее время наиболее распространенными способами совершения дистанционных преступлений остаются:



ГУ МВД России по Челябинской области