Приложение 3

Наиболее распространенными схемами совершения мошеннических действий остаются:

1. Осуществление звонков с федеральных номеров («8800…», «8495…», номеров, принадлежащих федеральным органам власти РФ), а также с абонентских номеров от имени представителей крупных банков РФ, сотрудников правоохранительных органов под предлогом пресечения сомнительных операций по счетам, оформления кредита неизвестным лицом, получение мошенником сведений о сроке действия и cvc-кода гражданина.
2. Осуществление звонка от имени оператора сотовой связи, который поясняет, что у гражданина заканчивается срок действия сим-карты, для продления срока действия сим-карты, необходимо сообщить код подтверждения из поступивших на абонентский номер текстовых сообщений, в дальнейшем злоумышленник включает переадресацию вызовов и осуществляет вход в «банкинг онлайн» с последующим списанием денежных средств.
3. Приобретение товара через сайты бесплатных объявлений («Авито», «Юла», «Дром» и т.д.), где злоумышленник поясняет, что товар есть в наличии, однако для его получения необходимо произвести либо стопроцентную предоплату, или половину стоимости товара, если указана крупная сумма оплаты.
4. Приобретение товара, либо заказ услуги через группы социальных сетей «Вконтакте», «Инстаграмм», группы в «Telegram, WhatsApp, Viber», где гражданину предлагается сначала внести стопроцентную предоплату, после которой он получит свой товар, либо запись на необходимую услугу.
5. Поиск товара через поисковые системы сети Интернет, где гражданин попадает не на официальный сайт продажи товара, а на фишинговый сайт (дубликат) с измененным расчетным счетом и контактными данными продавца.
6. Займы в микрофинансовых организациях.
7. Мошенничество при инвестировании.