Основные виды преступлений в сфере информационно-телекоммуникационных технологий, зарегистрированные в УМВД России по г.Сургуту

1. Звонок от имени оператора сотовой связи, который поясняет, что у гражданина якобы заканчивается срок действия сим-карты, а для продления срока действия сим-карты необходимо сообщить код подтверждения из поступивших на номер телефона текстовых сообщений. Далее злоумышленник включает переадресацию вызовов и осуществляет вход в «банкинг онлайн» с последующим списанием денежных средств.

2. Звонок с федеральных номеров («8800…», «8495…» с номеров принадлежащих федеральным органам власти РФ), а также с абонентских номеров: мошенник представляется сотрудником одного из банков РФ (так же якобы в данном мероприятии участвуют сотрудники правоохранительных органов, следственного комитета, прокуратуры и ФСБ), поясняет гражданину, что его карта заблокирована, или по банковской карте происходит не санкционированное списание денежных средств, либо несанкционированное оформление кредита, с осуществлением входа в личный кабинет «банкинг онлайн», либо перемены абонентского номера привязанного к банковской карте, при этом гражданину поступают смс-сообщения от банка с кодом о проведения любых операций.

3. Бронирование отелей (гостевых домов, квартир) по месту проведения отпусков. Злоумышленники создают сайты (форумы, группу в соц. сетях, в Интернет объявлениях) и указывают условия бронирования такие как: предоплата, оплата после подтверждения с бесплатной отменой в любой момент. Что бы не попасться на уловки, необходимо: пользоваться проверенными сервисами, читать отзывы, связаться со службой поддержки, не перечислять денежные средства на электронные кошельки и банковские карты.

4. Бронирование поездок через приложение «blabla car». Злоумышленники под видом водителей создают профили, и для оплаты поездки просят пройти по ссылке якобы от приложения «blabla car» (безопасная сделка). Нельзя переходить по ссылке, оплата только лично водителю при встрече на обусловленном месте.

5. Приобретение товара, либо заказ услуги через группы социальных сетей «Вконтакте», «Инстаграмм» группы в «Telegram, WhatsApp, Viber» где гражданину предлагается сначала внести стопроцентную предоплату, а после он получит свой товар, либо запись на необходимую услугу, а так же, получение сообщения от человека, который находится в «друзьях» в социальных сетях, с просьбой о том, что ему срочно нужны денежные средства, ссылаясь на то, что он потом все объяснит и просит сумму денежных средств с предоставлением банковской карты, куда необходимо перечислить денежные средства.

6. 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 выслать либо стопроцентную предоплату, или половину стоимости товара, если указана большая сумма оплаты, может выслать гражданину, по просьбе последнего, его фото, либо товарно-транспортную накладную о том, что товар действительно находится в одной из транспортной компании с чеком об оплате.

7. Поиск товара через поисковые системы сети Интернет, где гражданин попадает не на официальный сайт продажи товара, а на фишинговый (дубликатный) сайт, где размещается одинаковая информация, размещаемая и на официальном сайте, с изменением расчетного счета перечисления денежных средств, а также контактных данных.