ИНФОРМАЦИЯ
о наиболее распространенных способах и видах преступлений в сфере информационно-телекоммуникационных технологий, совершаемых в отношении жителей Ямало-Ненецкого автономного округа

1. **Звонки и сообщения от имени представителей госструктур.**

Злоумышленники, представляясь сотрудниками службы безопасности банков, правоохранительных органов, под предлогом пресечения несанкционированного списания денежных средств и оформления кредита, убеждают граждан оформить кредит и перевести заёмные денежные средства на указанные злоумышленниками номера банковских карт, счета абонентских номеров (в том числе «защищенные»), расчетные счета, электронные кошельки.

2. **Совершение мошенничеств с использованием специальных программ удаленного доступа к устройству.**

Злоумышленники под предлогом пресечения мошеннических действий с денежными средствами потерпевших убеждают их установить на мобильные телефоны приложение по удаленному доступу к устройству (Anydesk, TeamViewer, PC Remote, RMS, AirDrope и др.). После установки такого приложения преступники получают полный контроль над мобильными устройствами граждан и самостоятельно оформляют кредиты с последующим перечислением заёмных денежных средств на подконтрольные им счета.

3. **«Взлом» аккаунтов «ВКонтакте», «Одноклассники.ру», «Telegram» и др.**

Потерпевшие в результате недостаточной цифровой грамотности предоставляют злоумышленникам различными способами (как правило, пройдя по ссылке) логины и пароли от своих аккаунтов в социальных сетях (ВКонтакте, Одноклассники.ру, Telegram и др.). Мошенниками от имени потерпевших осуществляется рассылка списку его контактов, друзьям с просьбой одолжить денежные средства под различными предлогами (заболел родственник, не хватает на срочную покупку и т.д.) с указанием реквизитов банковской карты (счета).

4. Операторы сотовой связи.

Злоумышленники под видом операторов известных телекоммуникационных кампаний (сотовая связь) звонят жертве и сообщают, что нужно обновить договор или актуализировать данные, иначе номер будет заблокирован. Просят «всего лишь» продиктовать код из SMS, после чего получают доступ к аккаунту человека на «Госуслугах», либо полный удаленный доступ к устройству, после чего оформляют от имени граждан кредиты.

5. Кража мобильных номеров.

Злоумышленники крадут мобильные номера граждан с помощью подмены или восстановления eSIM (виртуальная SIM-карта). Получив доступ к телефону человека, они могут зайти в онлайн – банк и вывести деньги или даже взять кредиты на его имя, так как они могут проходить двухфакторные проверки через SMS для любых приложений, в том числе банковских сервисов, мессенджеров и социальных сетей.

6. Оплата услуг по фейковому QR-коду.

Злоумышленники используют поддельные платежные документы с QR-кодом в почтовый ящик. При открытии QR-кода списываются деньги.

7. Нажива на спецоперации и госизмене.

Злоумышленники придумывают легенды: найти пропавших родных или помочь им с лечением, призывают скидываться на нужды участников специальной военной операции, перечислив средства, отправив SMS на короткий номер.

8. Звонки по видеосвязи из банка в социальных мессенджерах.

Злоумышленники звонят по видеосвязи в социальных мессенджерах (WhatsApp, Viber и др.), где на экране вместо фотографии виден логотип одного из банков, после чего снимают лицо, чтобы затем использовать его для входа по биометрии (по изображению лица, радужной оболочке глаза и т.д.).

9. Использование злоумышленниками торговых интернет площадок, социальных сетей (Авито, Юла, OZON, Wildberries, ВКонтакте, Instagram).

Мошенники совершают действия путём введения в заблуждение потерпевших относительно продажи какого-либо товара, сдачи в аренду жилого помещения или же оказания иных услуг.

К примеру, при покупке товара покупателю направляется кассовый чек с трек-номером отправления. По прибытии посылки покупатель вместо товара получает пустую коробку. Возможен иной вариант - после получения денег злоумышленник отменяет отправку товара, в итоге покупатель остаётся без денег и без товара.

Также мошенники путём создания интернет-сайтов и аккаунтов в социальных сетях, схожих с официальными (dodopizza.ru, booking.com, skyscanner.ru, Сбербанк, ВТБ 24 и др.), принимают заявки от клиентов либо присылают сообщения со специально созданной ссылкой, при открытии которой пользователь перенаправляется на якобы платежную страницу банка для оплаты товара. Далее при введении данных своей банковской карты у лица списываются все имеющиеся на ней деньги.

10. Дополнительный заработок на инвестиционной бирже.

Гражданин находит в сети Интернет биржевую площадку по торговле криптовалютой (Binanace, Gartex, Kraken т.д.). После регистрации на указанной площадке, с гражданином связывается преступник, который предлагает высокий доход от покупки криптовалюты. Для этого необходимо открыть счет, а затем пополнить его на небольшую сумму (от 5-10 тысяч рублей) для приобретения и перепродажи крипто валюты. При этом злоумышленники убеждают клиентов передать им логин и пароль от счета (крипто-кошелька) для контроля и сопровождения операций по счету. Выплатив клиенту определенный доход от минимальных вложений, ему предлагается пополнить счет на более значительную сумму (от 500 тысяч рублей и более) для получения более высокого дохода. После пополнения счета гражданин лишается доступа к крипто-кошельку и своим деньгам.

МЕРЫ ПРЕДОСТОРОЖНОСТИ:

Алгоритм действий граждан по предупреждению совершения преступлений с использованием информационно-телекоммуникационных технологий:

1. При поступлении сомнительных телефонных звонков незамедлительно прекратить телефонный разговор, ни в коем случае не перезванивать.

2. При необходимости лично посетить отделение банка либо позвонить по телефону горячей линии кредитного учреждения, указанного на оборотной стороне банковской карты, а также в правоохранительные органы для получения соответствующих разъяснений.

3. Никому не сообщать свои персональные данные, данные банковских карт, коды, поступающие на телефон в СМС-сообщениях и мессенджерах.

4. Не переводить денежные средства на незнакомые счета.

5. Не устанавливать неизвестные приложения, в том числе по просьбе посторонних лиц.

6. Не инвестировать на неизвестных сайтах. Обращаться непосредственно в отделения кредитных учреждений при желании получения дохода от вложений в ценные бумаги и другие финансовые инструменты.

7. Не заполнять анкеты со своими персональными данными (паспортные данные, реквизиты банковских карт и т.д.) при посещении интернет-сайтов.

8. Не переходить по неизвестным ссылкам для проведения оплаты.

9. Не вносить предварительную оплату за товар или поездку, а также не производить оплаты за кого-либо.

10. В социальных сетях, аккаунтах мессенджеров, онлайн кабинетах устанавливать сложный пароль, многоуровневую защиту (двухфакторная аутентификация), пользоваться антивирусными программами.

11. В случае возникновения сомнений в правильности совершения тех или иных действий незамедлительно обращайтесь в отделение банка либо правоохранительные органы для получения соответствующих разъяснений.

Отдел ОДУУП и ПДН УМВД России