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

1. Использование личного кабинета на портале «Госуслуги».

Злоумышленники, получив доступ к личному кабинету потерпевшего, похищают его персональные данные (паспорт, номер СНИЛС, ИНН и т.д.), после чего оформляют договоры кредитования в различных кредитно-финансовых учреждениях. Также, похищенные с портала «Госуслуги» персональные данные могут быть проданы иным лицам для совершения в дальнейшем мошеннических действий.

*Пример: Потерпевшему Иванову И.И. поступает звонок на мобильный телефон с абонентского номера 8-495-***-**-**. Лицо, осуществляющее звонок, представляется сотрудником портала «Госуслуги» и сообщает Иванову И.И. о том, что совершена попытка взлома его личного кабинета.*

Для пресечения доступа неизвестных лиц к персональным данным Иванову И.И. предлагается сообщить конфиденциальные сведения в виде логина и пароля для входа в личный кабинет. Потерпевший, не подозревая о том, что звонящий ему человек является мошенником, сообщает свой логин и пароль для входа в личный кабинет. Преступник получает доступ в личный кабинет потерпевшего, где используя его персональные данные (паспорт, СНИЛС, ИНН), заказывает выписку справки «2-НДФЛ» (с целью установления доходов потерпевшего), а также выписку из бюро кредитных историй. Получив указанные данные, злоумышленник оформляет на имя Иванова И.И. договоры кредитования в различных кредитно-финансовых учреждениях.

2. Получение доступа к аккаунтам в социальных сетях и мессенджерах, приложениях «WhatsApp», «Telegram» и т.п.

Злоумышленники, получив временный доступ к учетным данным потерпевшего (аккаунту) в мессенджерах «WhatsApp», «Telegram» и т.п., осуществляют рассылку сообщений друзьям, родственникам и членам семьи с просьбой об одолжении денежных средств под различными предлогами на указанные ими банковские счета.

Пример: Злоумышленник устанавливает на принадлежащий ему телефон приложение «WhatsApp». Далее злоумышленник в позднее время суток осуществляет запуск установленного приложения. При осуществлении запуска приложения преступник вводит не свой номер, а номер сотового телефона Иванова И.И.

При запуске приложения администрация «WhatsApp» отправляет на номер сотового телефона Иванова И.И. коды и пароли для регистрации и использования приложения. Коды поступают Иванову И.И., но он их не замечает ввиду ночного времени суток.

Мошенник устанавливает приложение на свой телефон, указывая абонентский номер телефона Иванова И.И. более 3 раз. Администрация

приложения «WhatsApp» 3 раза направляет Иванову И.И. коды и пароли, но не получив от Иванова И.И. подтверждение, блокирует учетную запись Иванова И.И. на 12 часов в связи с подозрительной активностью.

После чего, злоумышленник направляет в администрацию приложения электронное обращение от имени Иванова И.И. с жалобой на то, что его учетную запись в «WhatsApp» заблокировали, с просьбой выслать новый пароль на адрес электронной почты, принадлежащий мошенникам.

При получении обращения администрация приложения сбрасывает преступнику коды доступа к приложению на указанный в обращении электронный адрес.

Злоумышленник вводит пароль, высланный администрацией «WhatsApp», в приложение, установленное на его телефоне, но с абонентским номером Иванова И.И., таким образом получает доступ ко всем его контактам.

Далее мошенник начинает рассылку СМС-сообщений всем контактам Иванова И.И. В сообщениях обращается к контактам с просьбой об одолжении денежных средств с указанием счетов, на которые нужно осуществить перевод. Контакты Иванова И.И., получив СМС-сообщения, переводят денежные средства мошенникам по указанным реквизитам, будучи уверенными, что сообщение пришло именно от Иванова И.И.

3. Совершение мошеннических действий посредством мобильной связи, социальной сети «WhatsApp» и других мессенджеров.

В указанных случаях злоумышленники, представляясь сотрудниками службы безопасности банков, правоохранительных органов, под предлогом пресечения несанкционированного списания денежных средств и оформления кредита убеждают граждан оформить кредит и перевести денежные средства на указанные злоумышленниками номера банковских карт, счета абонентских номеров, расчетные счета, электронные кошельки.

При этом мошенники владеют персональными данными потерпевших, называют их фамилию, имя, отчество, дату рождения, номера банковских счетов, адрес проживания, номера телефонов, паспортные данные и т.д., тем самым вызывая к себе доверие.

Как правило, телефонные звонки гражданам поступают с «подменных» номеров, то есть на дисплее телефонов граждан отображаются действующие номера сотрудников правоохранительных органов, прокуратуры, Федеральной службы безопасности, сберегательного банка, в том числе номер «900».

«Подменный» номер создается при помощи специальных программ, звонок осуществляется не с помощью сотовой связи, а посредством сети Интернет. Информацию о номерах телефонов правоохранительных органов и кредитных организаций мошенники узнают из официальных сайтов и подменяют при звонке.

Мошенники звонят гражданину с территории Украины, при этом на дисплее высвечивается номер сотрудника следственного отдела Главного

Управления МВД России по г. Москве, который имеется на официальном сайте МВД России.

Злоумышленники при общении с гражданами излагают «легенду», сообщая, что на имя гражданина неизвестными лицами оформляется кредит.

В ходе разговора злоумышленники под различными предлогами в корыстных целях убеждают потерпевших оформить максимально возможное количество кредитов в различных банках, чтобы уменьшить кредитный потенциал гражданина, с целью не дать возможности неизвестным лицам оформить на их имя кредит.

Далее мошенники просят перевести деньги посредством личного онлайн кабинета на «защищенный личный счет», который фактически принадлежит мошенникам либо направляют граждан к банкомату или в офис банка для снятия денежных средств с карты или счета для последующего внесения их на якобы «защищенный личный счет».

При этом, мошенники убеждают потерпевших не контактировать с сотрудниками службы безопасности банков, правоохранительных органов, прокуратуры, Федеральной службы безопасности и т.д., убеждая граждан, что проводится специальная операция по поимке преступников, а указанные должностные лица являются сообщниками преступников, оформляющих незаконный кредит на имя потерпевших.

Злоумышленники находятся в постоянном контакте с потерпевшими, торопят их с принятием решения, чтобы у граждан не было возможности посоветоваться с близкими родственниками, знакомыми, а также обдумать свои действия или сообщить в правоохранительные органы.

После перевода денежных средств в личном кабинете либо через банкоматы, денежные средства поступают на банковские счета злоумышленников.

Характерный пример: На абонентский номер 8918....000 гражданина Иванова И.И. поступило 8 вызовов, в том числе с номера «900», «88005678921», «8495556678912», стационарных абонентских номеров с кодами ЯНАО, в мессенджере «WhatsApp» с неустановленного номера, при звонке с которого, отображался логотип Сбербанка.

Звонившие представлялись сотрудниками службы безопасности Сбербанка, сотрудниками следственного комитета г. Москвы. Указанные лица сообщили Иванову И.И., что в отделении Сбербанка г. Москвы на его имя некий Петров П.П. пытается оформить кредит в сумме 1 миллион рублей. При этом мошенники сообщили, что по данному факту ими проводится «специальная операция», о которой Иванову И.И. нельзя сообщать никому, в том числе сотрудникам правоохранительных органов (МВД, ФСБ, СКР, прокуратура), а также сотрудникам банка, расположенного по его месту жительства, так как возможно в данной махинации задействованы обозначенные должностные лица.

Далее Иванову И.И. предложили оформить в Сбербанке максимальный кредит, чтобы Петрову В.В. отказали в получении кредита из-за превышения кредитного лимита.

Действуя по указанию злоумышленников, Иванов И.И. в личном кабинете «Сбербанк онлайн» под диктовку преступников оформил заявку на получение кредита в максимально возможной сумме - 1.5 миллиона рублей. После одобрения заявки мошенники сказали Иванову И.И. проследовать в ближайший банкомат и перевести деньги на указанные мошенниками «защищенные безопасные счета», созданные Сбербанком специально на имя Иванова И.И., убедив, что таким образом Иванов И.И. спасет свои деньги и в последующем по своему усмотрению распорядится оформленным кредитом.

После перевода денежных средств связь с потерпевшим прекратилась, телефонные номера звонивших оказались заблокированы. В результате проведенной махинации Иванов И.И. остался без денег с оформленным кредитом на 1,5 миллиона рублей.

4. Совершение мошенничеств с использованием специальных программ удаленного доступа к устройству.

Злоумышленники под предлогом пресечения мошеннических действий с денежными средствами потерпевших убеждают их установить на смартфон 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 на них кредиты с последующим перечислением заёмных денежных средств на подконтрольные им счета.

5. 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.

6. 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.

7. Дополнительный заработок в сети Интернет (финансовые пирамиды, инвестиции).

В сети Интернет (ВКонтакте, Instagram, Одноклассники.ру, YouTube, Telegram и т.д.) гражданин находит информацию о дополнительном заработке путем инвестирования, вложения средств в виде приобретения акций различных крупных корпораций.

После регистрации с лицом связывается мошенник, который предлагает высокий пассивный доход от инвестирования в ценные бумаги. Для этого предлагается гражданам открыть счет, а затем его пополнить (на сумму от 50 тысяч рублей и более) с целью приобретения и перепродажи акций крупных торговых корпораций. При этом злоумышленники убеждают клиентов передать им логин и пароль от счета для контроля и сопровождения операций по счету. Выплатив клиенту определенный доход от минимальных вложений, ему предлагается пополнить счет на более значительную сумму (от 1 миллиона рублей и более) для получения более высокого дохода. После пополнения счета гражданин лишается доступа к крипто-кошельку и своим деньгам.

8. Заказ такси в BlaBlaCar.

Злоумышленник размещает в приложении BlaBlaCar либо на сайтах-двойниках объявление о совместной поездке. Для оплаты за проезд мошенники направляют клиентам специально созданную ссылку. Произведя оплату по данной ссылке путём введения данных банковской карты, у потерпевшего одновременно списываются все хранящиеся на банковском счете денежные средства. Также при бронировании места в автомобиле на сайте BlaBlaCar мошенники направляют клиенту ссылку для оплаты брони. В дальнейшем при её оплате мошенники на связь не выходят, номер телефона гражданина блокируют.

Правила безопасного поведения граждан, направленные на предупреждение мошеннических действий:

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.

По всем возникающим вопросам, связанным с противодействием преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, обращаться в управление уголовного розыска Управления МВД России по Ямало-Ненецкому автономному округу по телефону: 7-62-84 (Ясавиев Айрат Фаритович).