***Актуальные способы совершения мошеннических действий на территории Ненецкого автономного округа***

- ***Схема с «продлением текущего договора на обслуживание сим -карты»***

*Аферисты обращаются к гражданам России с утверждением о необходимости как можно быстрее продлить договор на пользование телефонным номером, а не то в противном случае документ будет аннулирован и номер перейдет другому человеку. Во время такого разговора злоумышленник старается максимально отвлечь внимание потенциальных жертв, рассказывая о различных технических деталях. Далее мошенник уточняет, на какой срок человек желает продлить договор с мобильным оператором. После получения всей необходимой информации на телефон жертвы приходит SMS-сообщение с кодом подтверждения, который необходимо сообщить «для подтверждения пользовательского соглашения» о продлении договора на новый срок и прохождения полной верификации через личный кабинет портала «Госуслуг». В процессе разговора мошенник продолжает отвлекать собеседника различными ненужными деталями, невзначай спрашивает код, который пришел в сообщении, а затем говорит о том, что отправил клиенту ссылку. По этой ссылке жертве предлагается перейти и ввести код для завершения «дистанционного подписания договора». Этот код, в большинстве случаев, является кодом подтверждения для авторизации в личном кабинете потенциальной жертвы на портале «Госуслуг», либо кодом доступа к личным кабинетам кредитных учреждений пользователя. К тому же злоумышленники могут также попросить человека внести на телефонный номер с помощью банковской карточки небольшую сумму денег, предложив сделать это на сайте по указанной ими ссылке. В результате этого в руках аферистов окажутся и платёжные данные пользователя.*

*В реальности подобные договора с операторами связи, которые заключаются между телеком-компанией и физическими лицами, как правило, не предусматривают каких-либо ограничений по сроку пользования выбранным телефонным номером.*

*Также в настоящее время в России (в Ненецком автономном округу зарегистрирован 1 факт) данная схема получила своё продолжение, а именно после получения доступа к личному кабинету интернет портала «Госуслуги» гражданам поступает звонок якобы от представителей Центрального банка либо сотрудников силовых структур, которые сообщают о неправомерном доступе к личному кабинету пользователя интернет портала «Госуслуг», далее помогают восстановить доступ к личному кабинету, называя ему секретное слово, которое было установлено мошенниками ранее. После восстановления доступа лже-сотрудники Центрального Банка сообщают о том, что неизвестными лицами получена информация касающаяся дохода лица (справки 2-НДФЛ, кредитная история) и от его имени направлены заявки в кредитные учреждения на получения кредитов. С целью спасти свои денежные средства и для предотвращения получения мошенниками кредитов гражданину советуют самостоятельно обратится в кредитные учреждения с целью исчерпать свой*

*кредитный потенциал и направить денежные средства временно на «безопасный счет Центрального банка».*

- ***Схема со «звонком (смс сообщением) руководителя»***

*Злоумышленники разработали способ выманивания денежных средств у доверчивых россиян. Они выдают себя за руководителей различных организаций, силовых структур, главврачей больниц и других ответственных лиц.*

*Мошенники стали активно подделывать официальные аккаунты руководителей в сервисах обмена сообщениями. После этого, используя поддельные учетные записи, они связываются с подчиненными тех лиц, чьи страницы были подделаны. В ходе общения, лжедиректор предупреждает своего сотрудника о том, что ему скоро якобы поступит звонок от государственной структуры, например, из Банка России, Генеральной прокуратуры, ФСБ или полиции. Злоумышленник утверждает, что для организации этот звонок критически важен, и сотрудник должен строго следовать инструкциям звонящего. Кроме того, мошенник настаивает на том, что о данном разговоре сотруднику не стоит сообщать даже своим близким. Таким образом, пытаясь усыпить бдительность жертвы этим предварительным звонком, злоумышленники в дальнейшем пытаются выманить у потенциальной жертвы денежные средства, ее персональные и платежные данные.*

- ***Схема с получением быстрого заработка***

*В мессенджеры стали приходить предложения о высоких заработках за пустяковую работу - оценить те или иные отели.*

*Предложение высокой зарплаты за примитивную и не требующую специальной квалификации работу - признак того, что вас хотят обмануть. Причем тот перечень действий, который предлагают осуществлять мошенники, и работой назвать сложно.*

*Однако такая попытка получить солидный заработок чревата потерями. Мошенники обязательно спросят реквизиты карты, на которую нужно "переводить" деньги, а также пришлют ссылку для регистрации у работодателя, пройдя по которой человек поможет мошенникам в доступе на свой аккаунт на портале Госуслуг.*

- ***Схема со звонками от представителей Центрального банка, сотрудников правоохранительных органов, с целью сохранения денежных средств и перевода их на безопасный (защищенный) счет.***

*В рамках этой схемы преступники предлагают гражданам перевести свои деньги на так называемые “безопасные счета”, обещая впоследствии возврат средств через «приемные» Центрального банка РФ.*

*Злоумышленники под различными предлогами убеждают граждан перевести свои средства на эти “специальные” счета, утверждая, что таким образом средства якобы будут защищены от мошенников. Для придания большей убедительности своим словам, аферисты заявляют, что любая сумма,*

*переведенная на такой счет, может быть получена человеком лично в приемной Центрального банка РФ. Если потенциальная жертва идет на поводу у телефонных аферистов, то мошенники «записывают её на приём», а затем приходит SMS-сообщение с подтверждением записи с номера 300, который действительно принадлежит Банку России.*

*В пресс-службе Банка России указали на то, что если гражданин самостоятельно не записывался на прием через официальный сайт или контактный центр финансового регулятора, но получил SMS о записи, такое сообщение следует игнорировать. Никаких «специальных» или «безопасных» счетов для физических лиц, якобы размещенных в Банке России, не существует. Следовательно, все средства, отправленные на такие счета, напрямую попадают к мошенникам.*

*Сотрудники Центробанка не взаимодействуют напрямую с физическими лицами: они не звонят гражданам, не отправляют им копии документов и не требуют совершать какие-либо операции со счетами. Более того, сотрудники ЦБ РФ никогда не запрашивают у граждан их личные или платежные данные.*

- ***Схема с использованием приложения с удаленным доступом***

*В рамках этой схемы злоумышленники убеждают пользователей загружать приложения, которые, как утверждают, необходимы для доставки заказанного товара, для улучшения работоспособность телефона, заработка в сети интернет, новых мессенджеров.*

*На деле такие мобильные приложения имеют вредоносное содержимое, которое позволяет хакерам красть конфиденциальные и учетные данные, денежные средства пользователей.*

*Схема функционирует следующим образом: злоумышленники создают поддельные объявления о продаже товаров и размещают их на популярных интернет-площадках. Если находится покупатель, заинтересовавшийся товаром и готовый его оплатить, злоумышленники предлагают ему перейти в популярный мессенджер для дальнейшего разговора. Там пользователю присылают ссылку на скачивание вредоносного приложения, с помощью которого, якобы, можно оформить доставку. Мошенники заверяют потенциальную жертву, что являются индивидуальными предпринимателями, поэтому для приобретения у них товара с доставкой необходимо загрузить специальную программу на свое устройство. Если пользователь соглашается и переходит по предложенной ссылке, ему открывается фейковая страница магазина приложений Google Play. Злоумышленники предлагают загрузить и установить приложение, которое имитирует дизайн и функции реальных интернет-площадок, маркетплейсов. Однако такие приложения являются фейковыми и заражены вредоносным ПО. После установки этого приложения пользователю предлагается оформить доставку. Если человек следует инструкциям злоумышленников, в момент оплаты вредоносное ПО перехватывает и отправляет на сервер злоумышленников все введенные данные с банковской карточки, а также код подтверждения из SMS-сообщения. В итоге*

*хакеры получают доступ к денежным средствам жертвы, а пострадавший покупатель так и не получает заказанный товар.*

- ***Схема с рассылкой спам-информации в различных мессенджерах (социальных сетях)***

*Схема функционирует следующим образом: злоумышленники пишут россиянам в мессенджер или в социальных сетях. Они сообщают, что ребенок якобы победил в каком-то конкурсе у известного блогера. Чтобы получить полагающийся приз, необходимо совершить некоторые действия с использованием телефона. Злоумышленники утверждают, что нужно предоставить определенную информацию с телефона, включая платежные данные, например, логин и пароль от онлайн банкинга. В ряде случаев мошенники просят сфотографировать банковскую карточку с обеих сторон.*

*В течение последнего года россиянам также стали часто приходит сообщения в социальных сетях и мессенджерах от якобы знакомых людей. В этих сообщениях человека просили проголосовать в конкурсе на сайте «за ребенка». Если пользователь переходил по этой ссылке, система просили ввести его учетные данные от мессенджера Telegram или какой-либо популярной социальной сети. После этого, вместо обещанного голосования, учётные данные отправлялись злоумышленникам, и аккаунт человека был скомпрометирован.*

***Как защититься от телефонных мошенников:***

*- При любом подозрительном звонке сразу класть трубку и не брать ее, пока ситуация не прояснится. Лучше тут же перезвонить на официальный номер кредитного учреждения.*
*- Прежде чем расплатиться в интернете, внимательно проверить домен, чтобы не стать жертвой фишинга.*
*- Крайне внимательно разрешать программам на смартфоне доступ к SMS и приему звонков, так как среди них может оказаться шпионское ПО, крадущее данные.*
*- Оформить eSIM, если это возможно на вашем телефоне, так как такой вариант безопаснее и удобнее стандартной SIM-карты.*
*- Никогда не спешить при переходе по ссылкам, где понадобятся персональные данные. После перехода нужно еще раз убедиться, что сайт настоящий.*
*- Преступники, создающие фишинговые ресурсы, похищают личную информацию, получают ответы на контрольные вопросы, «заражают» ваши устройства.*
*- Даже если какой-то файл прислали знакомые, нужно быть очень внимательным при его открытии. Самый частый способ «заражения» компьютера или смартфона – файл, который запустила сама жертва. Вирусы могут быть в файлах разного формата, а для обмана антивируса их тщательно шифруют.*

*- Пользоваться услугами надежных и крупных мобильных операторов. Посредством малоизвестных виртуальных операторов злоумышленники, промышляющие социальной инженерией, получают персональные данные.*
*- Помнить, что сотрудники служб безопасности и правоохранительных органов никогда сами не звонят по телефону в мессенджерах Telegram, WhatsApp, и не предлагают решить какие-либо вопросы, связанные с Вашими финансами, уголовным преследованием, по телефону.*
*- Насторожиться, если звонящий произносит фразы про лицевой счет, привязку карты к телефону и прочее.*
*Не говорить «да», отвечая на вопросы.*
*- Тщательно отслеживать речь и поведение собеседника, чтобы уловить подозрительные моменты.*
*- Прежде чем совершать любые действия, отставить панику и тщательно все проверить.*

***Самый действенный способ защиты своих персональных данных на интернет портале «Госуслуги»:***

*- создание сложного пароля (минимум 12 символов, не связанных с вами, не сохранять данный пароль в облачном хранилище мобильного телефона);*

*- подключение двухфакторной аутентификации (в разделе «Безопасность» выбрать вкладку «Вход в систему» выбрать «Вход с подтверждением») – при входе в приложение на Ваш мобильный номер сотовой связи будет приходит дополнительное смс с кодом, либо необходимо будет ввести ответ на секретный вопрос.*

В случае обнаружения мошеннических действий, либо если Вы стали жертвой мошенников, необходимо обратиться в УМВД России по Ненецкому автономному округа по адресу: г. Нарьян-Мар, ул. Выучейского, д. 13, по телефону 02, рабочий номер ОБК УМВД России по Ненецкому автономному округу 8-999-090-56-20.