Мошенники обманывают людей с помощью дипфейков

Признаки мошенничества	Что предпринять?
В России злоумышленники для хищения денег стали чаще использовать новый инструмент обмана — дипфейк-технологии. С помощью нейросети мошенники создают реалистичное видеоизображение человека. Затем сгенерированный образ рассылают его друзьям или родным через мессенджеры или социальные сети. В коротком фальшивом видеоролике виртуальный герой, голос которого иногда сложно отличить от голоса прототипа, рассказывает якобы о своей проблеме (болезнь, ДТП, увольнение) и просит перевести деньги на определенный счет. В некоторых случаях мошенники создают дипфейки работодателей, сотрудников государственных органов, известных личностей из той сферы деятельности, в которой трудится их потенциальная жертва. Чтобы создать цифровую копию конкретного человека, злоумышленники используют фото и видео, а также запись голоса, полученные в основном в результате взлома его аккаунта в социальных сетях или мессенджерах.	Проявляйте осторожность при получении от своего знакомого голосового или видеосообщения с просьбой о финансовой помощи — его аккаунт могли взломать злоумышленники. Иногда для рассылки таких сообщений мошенники создают поддельные страницы с именем и фото человека. Не спешите переводить деньги! Обязательно сначала позвоните тому, от чьего имени поступило сообщение, и перепроверьте информацию. Распознать дипфейк можно по неестественной монотонной речи собеседника, дефектам звука и видео, несвойственной мимике. Если возможности позвонить и убедиться, что человеку действительно нужна помощь, нет, задайте в сообщении личный вопрос, ответ на который знает только ваш знакомый.

Мошенники предлагают пересчитать пенсию из-за неучтенного стажа работы

Признаки мошенничества	Что предпринять?
Злоумышленники звонят пожилым людям и представляются работниками Социального фонда России (СФР). Они сообщают, что размер текущей пенсии можно существенно увеличить, так как будто бы обнаружен неучтенный трудовой стаж. Тех, кто поверил аферистам, приглашают якобы на консультацию в Многофункциональный центр или отделение СФР для решения вопроса. Причем мошенники называют настоящие адреса центров или отделений, которые находятся в городе, где живет потенциальная жертва. Это усыпляет бдительность человека. По сценарию злоумышленников, для записи на прием человек должен предоставить данные паспорта, СНИЛС, ИНН и назвать код из СМС-сообщения. На деле перечисленные документы и числовой код из сообщения нужны мошенникам для получения доступа к учетной записи человека на портале Госуслуги. Заполучив доступ к ней, они могут беспрепятственно оформить на жертву кредиты или займы.	При поступлении такого телефонного звонка прервите разговор. Настоящие сотрудники государственных служб, в том числе Социального фонда России, не звонят с подобными вопросами. По любым социальным вопросам нужно самостоятельно позвонить в единый контактный центр СФР по телефону 8-800-10-000-01 либо обратиться в ближайшее отделение фонда. Никому и никогда не сообщайте личные данные, реквизиты карт, СМС-код, а также логины и пароли от своих аккаунтов.

Мошенники стали обманывать военнослужащих и их родных

Признаки мошенничества	Что предпринять?
Злоумышленники обновили свою популярную схему про «безопасный» счет. Теперь они начали использовать ее в отношении военнослужащих либо их близких родственников. Мошенники звонят или пишут своим потенциальным жертвам и сообщают, что единовременная выплата в размере 195 000 рублей, которая причитается военным в соответствии с указом Президента РФ, будет удержана из денежного довольствия. Причина — дисциплинарное взыскание или нарушение при выполнении служебных обязанностей в зоне проведения специальной военной операции (СВО). Для большей убедительности злоумышленники направляют в мессенджер «копию выписки» якобы из приказа Департамента финансового обеспечения Минобороны России. По сценарию, придуманному мошенниками, военнослужащему или его родным, чтобы избежать списания денег и сохранить средства, предлагают перевести все накопления с карты на «безопасный» счет, а затем средства обещают вернуть. Однако, получив обманным путем деньги жертвы, телефонные аферисты исчезают.	При поступлении такого телефонного звонка прервите разговор. Если вам пришло подозрительное сообщение или письмо, не реагируйте на них. Следует помнить, что «безопасных» («специальных») счетов не существует. В действительности счет, реквизиты которого называют мошенники, принадлежит им. По любым вопросам, связанным с деньгами, самостоятельно обратитесь в свой банк по номеру телефона, указанному на его официальном сайте или на обороте платежной карты.

Как не стать жертвой мошенников: общие рекомендации

Не сообщайте никому и никогда паспортные данные и финансовые сведения: данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-код. Сотрудники банков и государственных структур никогда не запрашивают такую информацию. Не публикуйте ее в социальных сетях, на форумах и каких-либо сайтах в Интернете, а также не храните данные карт и PIN-коды на компьютере или в смартфоне.

Если с неизвестного номера звонит сотрудник Центробанка, правоохранительных органов, государственной организации или банка с сомнительным предложением (например, сообщением о попытке оформления кредита или подозрительной операции от вашего имени, обещанием высокого дохода по вкладу, предложением перевести средства на специальный счет Центробанка и тому подобное) или по телефону запугивают и требуют быстрых действий с финансами, положите трубку. Если подозреваете, что вам звонит мошенник, позвоните в банк по номеру телефона, указанному на обратной стороне карты или на его сайте, или в контакт-центр ведомства, сотрудником которого представлялся звонящий.

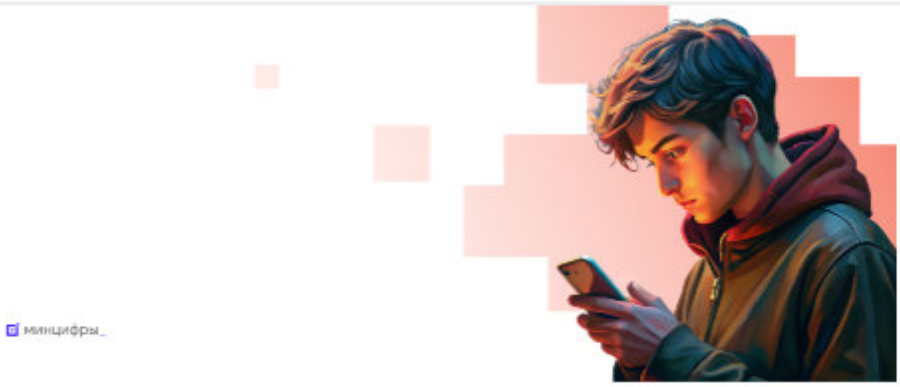
Не совершайте каких-либо действий по счету, если вам звонят из Центробанка с просьбой или требованием о переводе денег, в том числе на «защищенный» или «специальный» счет, или с предложением об оформлении кредита. Банк России не открывает счета и не работает с гражданами.

По возможности установите антивирус на все устройства и обновляйте его.

Совершайте покупки в Интернете только на проверенных сайтах. Заведите специальную карту для онлайн-покупок и пополняйте ее ровно на ту сумму, которая нужна для оплаты. При совершении покупок обращайте внимание на наличие в строке браузера рядом с названием сайта значка безопасного соединения (замочка).

Никогда не вводите личные и финансовые данные на сомнительных сайтах и не переходите по ссылкам из подозрительных писем, которые предлагают, например, пройти опрос, получить какую-либо выплату и тому подобное. Официальные сайты финансовых организаций в поисковых системах (Яндекс, Mail.ru) помечены цветным кружком с галочкой.

Как защититься от мошенников: простые правила Минцифры



Москва, 2 июля 2024 года – Схема действий злоумышленников всегда одинакова: обманным путём они вынуждают человека самостоятельно сообщить данные для входа в личный кабинет банковского приложения, мобильного оператора, Госуслуг и других полезных ресурсов. Чтобы звучать убедительно и воздействовать на эмоциональном уровне, они затрагивают самые актуальные темы.

Мошенники могут представляться сотрудниками социальных служб, медиками, правоохранителями, обещать выигрыш в лотерею или увеличение пенсии, выплаты от государства или выгодный кредит. Такие методы получения доступа к данным называются социальной инженерией.

Как защитить себя от социальной инженерии

— Будьте бдительны во время телефонных разговоров. Не торопитесь. Если диалог кажется вам подозрительным, прервите звонок. Лучше перезвоните в банк или организацию по номерам, указанным на официальном сайте. Помните, что представители Госуслуг и служб безопасности банков никогда не звонят первыми

— Обратите внимание на способ связи. Для звонков мошенники часто используют мессенджеры. Настоящие представители ведомств и органов власти никогда не будут звонить через WhatsApp или Telegram

— Не сообщайте никому логины и пароли от личных кабинетов. Внимательно читайте назначение смс-кодов. Например, смс-коды Госуслуг могут потребоваться только лично вам и никому больше. Не говорите никому ответ на контрольный вопрос, который вы используете для восстановления доступа.

— Внимательно следите за актуальностью номера, к которому привязан аккаунт

— Используйте сложные пароли, периодически меняйте их. Если сервис позволяет, подключите двухфакторную аутентификацию. На Госуслугах в качестве второго фактора можно выбрать смс-код, одноразовый ТОТР-код и вход по биометрии

— Внимательно изучайте адрес страницы, на которой вводятся данные, чтобы не попасть на фишинговый ресурс. Единственно верный адрес Госуслуг — gosuslugi.ru.

Госуслуги надёжно защищены, и злоумышленник может получить доступ к аккаунту только в том случае, если пользователь сам передаст всю необходимую для входа информацию. На портале есть все инструменты для того, чтобы обезопасить аккаунт. Но нужно бережно относиться к своим данным.