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.

Использование ложных аккаунтов руководителей Банка России в мессенджерах

Признаки мошенничества	Что предпринять?
Мошенники создают аккаунты в популярных мессенджерах от лица руководителей Банка России. Страницы содержат их реальные данные (фамилия, имя, отчество, фото — эти сведения берутся из Интернета) и выглядят максимально достоверно. Используя фальшивые аккаунты якобы служащих Банка России, злоумышленники отправляют сообщения руководителям или их заместителям различных крупных компаний или государственных органов. В письмах такие лжесотрудники просят помочь им, например, в задержании аферистов в кредитной организации и предупреждают о скором звонке уполномоченного сотрудника из профильного министерства. Они рекомендуют следовать инструкциям звонящего, а о факте разговора никому не рассказывать. После этого злоумышленники звонят потенциальной жертве и под различными предлогами пытаются получить доступ к банковским данным или убеждают добровольно перевести деньги на подконтрольные мошенникам счета. Такую схему злоумышленники могут применять и в отношении обычных граждан. Например, за счет создания поддельных аккаунтов друзей человека в социальных сетях.	Сотрудники регулятора не используют общедоступные мессенджеры или социальные сети для решения служебных вопросов. Обо всех подобных случаях мошенничества необходимо сообщать в правоохранительные органы. Банк России рекомендует гражданам сохранять бдительность и не сообщать посторонним людям личные и финансовые данные, под каким бы предлогом или каким бы способом их ни пытались узнать. Не нужно совершать какие-либо денежные операции по просьбе незнакомых лиц. При возникновении любых сомнений относительно сохранности денег на банковском счете необходимо самостоятельно позвонить в свой банк по номеру, указанному на его официальном сайте или на оборотной стороне банковской карты.

Злоумышленники стали похищать деньги без данных карты

Признаки мошенничества	Что предпринять?
Банк России выявил новую мошенническую практику социальной инженерии с применением QR-кода. Некоторые банки внедрили сервис снятия наличных денег с помощью QR-кода. В мобильном приложении клиент может самостоятельно сгенерировать такой код на нужную сумму, поднести его к сканеру в банкомате и снять наличные. Этим стали пользоваться злоумышленники. Они звонят клиентам банков под видом сотрудников кредитной организации, сообщают, что в банк поступил несанкционированный запрос на снятие денег со счета, и просят прислать QR-код, чтобы отменить операцию. Расчет на то, что потенциальная жертва не в курсе особенностей QR-кода и легкомысленно относится к изображению с черно-белыми квадратиками, поэтому легко может им поделиться. Заполучив код, лжесотрудники банков просто снимают деньги в банкоматах со счета обманутого человека.	QR-код в этом случае фактически является поручением банку на выдачу денег без ввода ПИН-кода. Никогда не делитесь QR-кодом с незнакомыми людьми, не храните его изображение в мобильных устройствах или в распечатанном виде. Помните, что настоящие сотрудники банков никогда не запрашивают у клиентов QR-код.

Мошенники представляются работодателями

Признаки мошенничества	Что предпринять?
Злоумышленники рассылают по электронной почте, через СМС или мессенджеры сообщения с привлекательными условиями работы: высокой оплатой труда, неполным рабочим днем, легкими задачами. Зачастую это работа на маркетплейсах (продажа товаров и услуг через Интернет). Для уточнения деталей человеку предлагают перейти по ссылке, которая ведет в популярные мессенджеры. Там с потенциальной жертвой вступают в переписку «менеджеры по подбору персонала». Они могут запросить у клиента данные банковской карты, номер мобильного телефона. Затем якобы для регистрации и активации аккаунта для работы на маркетплейсе требуется внести вступительный взнос — например, в размере 500 рублей. Но на самом деле эти деньги оседают в карманах мошенников, а данные банковской карты и номер телефона используются ими для попытки взлома личного кабинета человека на сайте банка и кражи средств с его счета.	Не доверяйте рассылкам с предложением о работе, тем более если вас заставляют оплатить какие-либо услуги, товары, зарезервировать вакансию и провести другие платежи. Такие предложения «гарантированной работы» — популярный прием мошенников. Кроме того, при получении таких предложений о работе не сообщайте свои паспортные данные и финансовые сведения (данные карты и ее владельца, трехзначный код с обратной стороны карты или СМС-код).

Сообщают клиенту банка об утечке персональных данных

Признаки мошенничества	Что предпринять?
Злоумышленники звонят гражданам и представляются сотрудниками правоохранительных органов. Вначале лжеполицейский сообщает человеку, что по поручению Центрального банка расследует дело о массовой утечке банковских данных, в числе которых могут быть и сведения о гражданине. Под таким предлогом и для возможного привлечения собеседника в качестве пострадавшего мошенник предлагает ему сверить банковские сведения с базой украденных данных. Далее злоумышленник спрашивает у человека, в каком банке он обслуживается, просит данные карты, в том числе трехзначный код на ее оборотной стороне. Чтобы убедить потенциальную жертву в правдоподобности истории, мошенник может направить в мессенджер или на электронную почту фото поддельного документа о проведении оперативно-розыскных мероприятий.	При поступлении такого телефонного звонка прервите разговор. Банк России напоминает, что ни работники банков, ни сотрудники правоохранительных органов никогда не запрашивают данные банковской карты (ее номер, трехзначный код с оборотной стороны, СМС-код). Эти сведения нужны мошенникам. Кроме того, ни Банк России, ни представители правоохранительных органов не направляют фото удостоверений или какие-либо другие документы.

Лжесотрудники Банка России

Признаки мошенничества	Что предпринять?
Банк России отмечает очередную волну широкого распространения мошеннической схемы, при которой злоумышленники представляются сотрудниками Центрального банка. Вначале мошенники звонят человеку и сообщают о сомнительных операциях, якобы совершаемых по счету или карте, после направляют ему в мессенджер или на электронную почту поддельное удостоверение сотрудника Банка России с логотипом и печатью. Такие документы могут содержать фамилии реальных работников — эти сведения злоумышленники могут брать с сайта регулятора. Высылая фальшивое удостоверение, они надеются убедить человека в правдоподобности своих недобросовестных действий, чтобы в дальнейшем лишить его денег или оформить на него кредит.	Банк России напоминает, что не работает с физическими лицами как с клиентами, не ведет их счета, не звонит им, а его сотрудники не направляют никому копии своих документов. При поступлении телефонного звонка от мошенника немедленно прервите разговор и по возможности заблокируйте его номер. При возникновении любых сомнений относительно сохранности денег на вашем банковском счете самостоятельно позвоните в свой банк по номеру, указанному на его официальном сайте или на оборотной стороне банковской карты.

Обмен кешбэка на рубли

Признаки мошенничества	Что предпринять?
Злоумышленники обзванивают граждан под видом сотрудников банков и сообщают, что накопленный за покупки кешбэк и другие бонусные баллы можно обменять на рубли. Для этого мошенники запрашивают у человека банковские данные и СМС-код, полученный от банка, якобы для подтверждения операции и оплаты комиссии за услугу. Однако на самом деле злоумышленники, заполучив эти сведения, совершают кражу денег со счета.	При поступлении такого телефонного звонка прервите разговор. Сотрудники банков никогда не запрашивают по телефону финансовые данные, в том числе трехзначный код с оборотной стороны карты или СМС-код. По любым банковским вопросам, в том числе по кешбэку, самостоятельно позвоните в банк по номеру, указанному на оборотной стороне карты или на сайте кредитной организации.

Обещают помочь с компенсацией похищенных денег

Признаки мошенничества	Что предпринять?
Чтобы якобы вернуть пострадавшему похищенные у него деньги, мошенники создают специальные сайты, ссылки на которые направляют по электронной почте, через смс или мессенджеры. Иногда они звонят с предложением оформить компенсацию за похищенные средства. Только за май 2022 года Банк России направил в правоохранительные органы на блокировку данные о 38 интернет-ресурсах с предложением различных компенсаций, а также возврата украденных мошенниками денег. Доверчивых граждан злоумышленники просят заполнить форму с личными и финансовыми данными, чтобы якобы проверить полагающуюся сумму возврата и оформить его. А затем, получив эти данные, похищают у человека деньги.	Клиент банка вправе рассчитывать на возврат похищенной суммы лишь в том случае, если он самостоятельно не переводил деньги на мошеннические счета и не раскрывал злоумышленникам свои личные и финансовые данные. Если деньги списали без вашего согласия, то единственный законный механизм вернуть их следующий: незамедлительно обратитесь в банк, заблокируйте карту и в течение суток после происшествия напишите в отделении банка заявление о несогласии с операцией.

Предлагают проверить данные счета на предмет утечки

Признаки мошенничества	Что предпринять?
Злоумышленники предлагают гражданам проверить, не попали ли данные счета или карты в руки третьих лиц. Для этого человеку присылают по электронной почте или иным способом ссылку на сайт, якобы проверяющий утечку банковских сведений. Как только жертва введет на этом сайте свои банковские данные, они оказываются у настоящих мошенников. После этого злоумышленники могут похитить деньги держателя карты или использовать его данные в противоправных целях.	Не существует сайтов, на которых можно проверить факт утечки банковских сведений! Никогда не вводите данные своего счета или карты (номер, срок действия, проверочный код с оборотной стороны карты) и персональные данные (данные паспорта, дату рождения, адрес местожительства и другие) на сомнительных сайтах, не переходите по ссылкам из подозрительных электронных писем или СМС-сообщений.

Убеждают оформить кредит

Признаки мошенничества	Что предпринять?
Человеку звонит якобы сотрудник бюро кредитных историй и утверждает, что на него или его близких родственников мошенники пытаются оформить кредит.	При поступлении такого телефонного звонка немедленно прервите разговор.
Через короткое время ему снова звонят и уже могут представляться сотрудниками службы безопасности банка, правоохранительных органов или Банка России. Звонящий подтверждает, что на имя гражданина или его близких неизвестные лица действительно оформляют кредит и, чтобы предотвратить его незаконное оформление, необходимо как можно скорее оформить «встречный» кредит самостоятельно онлайн или в офисе банка. Сумма кредита должна совпадать с той суммой, которую оформляют неизвестные лица по его паспортным данным.	Ни сотрудники банков, ни бюро кредитных историй не информируют граждан об изменениях в кредитной истории по телефону.
Для убедительности злоумышленники просят гражданина действовать оперативно и ни в коем случае не рассказывать про оформление кредита и его целях кому-либо, так как проводится секретная операция по вычислению жулика из числа сотрудников банка. Они убеждают жертву, что ее действия позволят раскрыть преступника, а кредитная история останется чистой.	Сообщить по телефону или каким-либо другим способом о попытке оформления кредита могут, как правило, только мошенники.
Во время разговора звонящие узнают, услугами каких банков пользуется жертва, и, чтобы войти в доверие, интересуются, не теряла ли она документы, удостоверяющие личность, и не передавала ли кому-либо свои паспортные данные.	