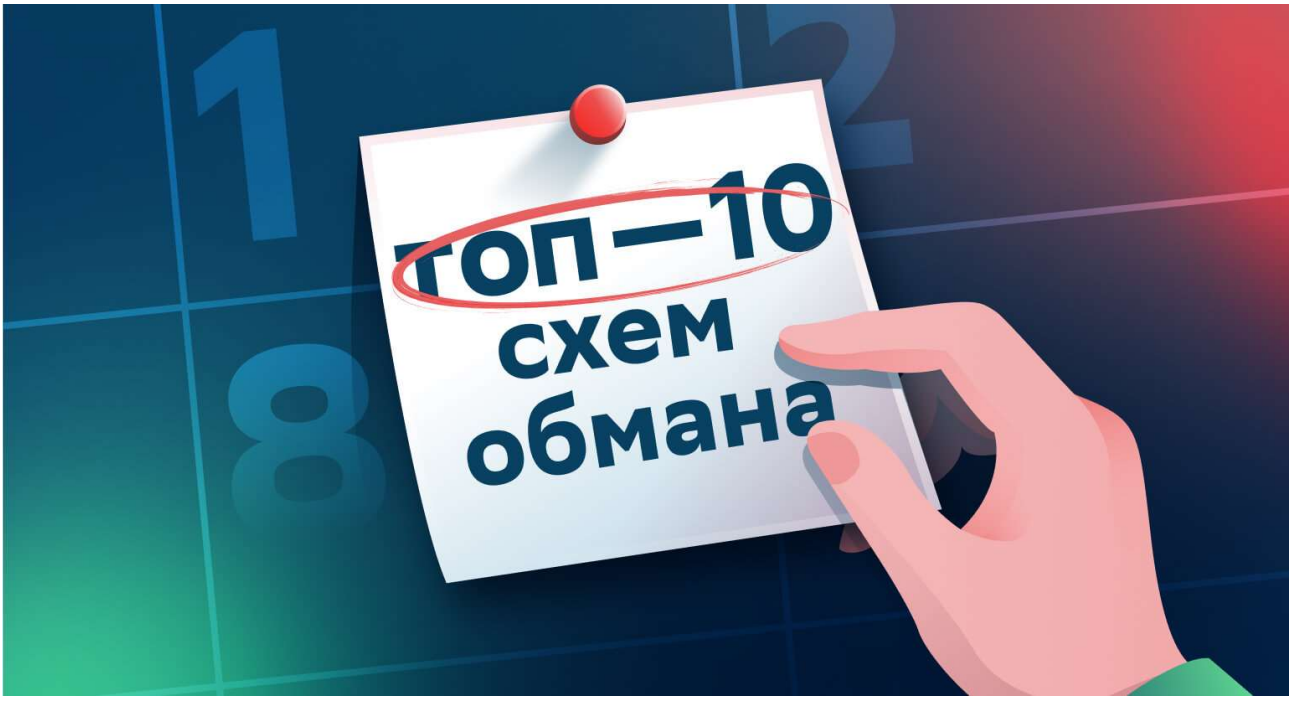
Топ-10 схем мошенников 2025 года

Мошенники продолжают придумывать всё более изощрённые способы обмана, используя социальную инженерию, психологическое давление и современные технологии. Какие схемы мошенничества наиболее популярны и как защититься от них?



1. <u>Украсть деньги через NFC: «бесконтактный обман».</u>

Мошенники всё чаще используют технологии бесконтактной оплаты для кражи средств с банковских карт. Они звонят жертве, представляясь сотрудниками банка или правоохранительных органов, и сообщают, что якобы взломаны Госуслуги, зафиксированы незаконные транзакции или жертва финансирует ВСУ.

Для «защиты» средств предлагают установить специальное приложение на смартфон. После этого жертву просят приложить свою банковскую карту к телефону и ввести PIN-код. При этом мошенники успокаивают жертву: карта остаётся у неё на руках, поэтому PIN-код вводить не опасно. На самом деле приложение считывает данные карты через NFC и передаёт их мошенникам, которые в этот момент находятся у банкомата. Злоумышленники прикладывает своё устройство с таким же приложением к терминалу банкомата. Терминал считывает устройство мошенника как карту жертвы, поэтому после ввода PIN-кода преступник получает доступ к её личному кабинету и может снять все деньги со счетов.

Бывают ситуации, когда мошенники действуют иначе:

Звонят с незнакомого номера или через мессенджеры и неожиданно сообщают шокирующую новость, например: «по вашему счёту зафиксированы незаконные транзакции» или «взломана ваша учётная запись на Госуслугах» и т. п. Мошенник стремиться запугать жертву и предлагает «спасти» денежные средства, установив на телефон специальное приложение. Направляет файл через мессенджер. Этот файл содержит вредоносное ПО, которое активируется на устройстве. После чего злоумышленник предлагает обналичить деньги со всех имеющихся счетов и внести их на специальный «безопасный счёт» через банкомат. Для этого надо приложить к банкомату телефон со включенным NFC сигналом.

Мошенник диктует цифры, с помощью которых, по его словам, жертва подтверждаете перевод на так называемый безопасный счёт. На самом деле это PIN-код от карты дропа, и человек сам вносит наличные на чужой счёт.

Установленная под воздействием мошенников специальная программа ретранслирует NFC-сигнал на устройство дропа. Банкомат считывает сигнал телефона как карту. И это позволяет злоумышленнику после ввода ПИН-кода, который выманивают обманом, войти в ваш личный кабинет и снять деньги со счета.

По данным компании F6, только за первый квартал 2025 года ущерб от таких атак составил 432 млн рублей.

Как защититься:

- Не устанавливайте приложения из непроверенных источников или по ссылкам из сообщений.
- Держите PIN-код в секрете, не вводите в приложениях, которые не являются официальными банковскими программами.
- Ограничьте использование NFC, включайте его только при необходимости и отключайте после использования.
- Установите антивирусное ПО на свой смартфон и регулярно обновляйте его.
- Будьте бдительны и не доверяйте незнакомым звонкам, особенно если вас просят установить приложения или предоставить конфиденциальную информацию.

2. «Спасти родителей».

Мошенники «целятся» в самых близких и дорогих нам людей. Под видом сотрудников полиции, ФСБ или Росфинмониторинга преступники звонят подросткам и сообщают страшную новость: родителям якобы грозит уголовное преследование за перевод денег за границу или незадекларированные доходы. Испугавшийся за маму или папу ребёнок готов на всё ради их спасения.

Злоумышленники требуют от детей провести «видеообыск» квартиры, показать на камеру все накопленные деньги и ценности, а затем передать их курьеру, чтобы «проверить» и «задекларировать». Такие совершённые под давлением действия приводят к потере семейных сбережений.

Так, в начале 2025 г. в Москве 14-летнего подростка заставили поверить в историю о «спасении родителей» и передать курьеру передать курьеру 300 тыс. рублей и иностранную валюту.

Как защититься:

- Объясните ребёнку, что ни один сотрудник полиции или госорганов не будет требовать деньги через курьера.
- Научите детей при любых тревожных звонках сразу обращаться к родителям.
- Установите правило: любые действия с деньгами и ценностями совершаются только после консультации с взрослыми.

3. «Служба доставки».

Злоумышленники звонят и представляются сотрудниками «Почты России», компании СДЭК или другой службы доставки. Сообщают, что на ваше имя пришло заказное письмо либо посылка из-за рубежа. Отследить заказ и выбрать адрес доставки якобы можно в специальном Telegram-боте. Мошенник либо присылает на него ссылку, либо диктует название бота по телефону. Телефонные мошенники убеждают, что этот чат необходим, так как через него будут приходить уведомления о статусе отправки/доставки заказных писем. Однако для авторизации в этом сервисе пользователь должен запустить Telegram-бот. А на самом деле в бот

встроена поддельная (фишинговая) форма для авторизации на Госуслугах. Если ввести по этой ссылке данные от аккаунта Госуслуг, мошенники получат к нему доступ. Они смогут взять на ваше имя микрозаймы или использовать доступ к вашей учётной записи для дальнейшего обмана.

Важный момент: при запуске Telegram-бота пользователь не видит поддельный (фишинговый) адрес сайта (ни с мобильного устройства, ни с версии Telegram для ПК). Этот адрес виден только при копировании ссылки из приложения в браузер, то есть фактически в момент перехода на фальшивую страницу авторизации на Госуслугах. В результате пользователь до последнего момента не понимает, что входит не в свой личный кабинет на Госуслугах, а на мошеннический ресурс.

Как защититься:

- Заходите в личный кабинет только через специальное приложение или веб-версию официального сайта.
- Отслеживайте заказы только в официальных приложениях или на сайте сервиса.

4. «Звонок на домашний телефон».

С 1 июня 2025 года в России введено новое правило: во время разговора по мобильному телефону пользователям больше не приходит СМС-код для авторизации на сайте «Госуслуги». Эта мера призвана снизить риски мошенничества, однако аферисты быстро адаптировались и изменили тактику.

Основные жертвы усовершеннствованной схемы — пожилые люди, которые реже используют интернет-сервисы, но доверяют звонкам на домашний телефон. Они считают, что знать их домашний номер могут только официальные организации.

Как работает схема

Мошенники звонят на домашний телефон, представляясь сотрудниками Ростелекома или другой известной организации. Повод для разговора может быть любым: продление услуги связи, подтверждение данных, технические работы. Злоумышленник, удерживая человека на связи на стационарном аппарате, просит назвать код из СМС, который приходит на мобильный телефон жертвы. Это нужно якобы для подтверждения операции. На самом деле этот код предназначен для входа на портал «Госуслуги». После передачи кода мошенники получают доступ к личному кабинету жертвы. Далее следует звонок от «государственных структур» — это может быть полиция, прокуратура, Центробанк. Сообщается, что из-за разглашения кода ваши деньги находятся в опасности, якобы они переводятся на счета экстремистских организаций или за границу. Для «спасения» средств и избежания уголовной ответственности предлагают срочно перевести все деньги на «безопасный счёт» или передать курьеру.

Как защититься:

- Никогда не называйте никому пароли и одноразовые коды подтверждения из СМС.
- Сотрудники операторов связи, служб доставки, поликлиник, государственных организаций и других организаций не запрашивают такие данные по телефону.
- Всегда уточняйте информацию через официальные контакт-центры организаций, от имени которых вам звонят.
- Не поддавайтесь панике и не принимайте поспешных решений под давлением.

5. «Цифровое мошенничество с медкартами».

Злоумышленники звонят гражданам и выдают себя за сотрудников медицинских учреждений, заявляя, что бумажные медицинские карты вскоре будут аннулированы в связи с модернизацией системы здравоохранения. Они сообщают, что карты будут переведены в цифровой формат, и предлагают доверчивым жертвам передать личные данные — номер СНИЛС и специальный код из СМС - сообщений.

Получив необходимые сведения, злоумышленники захватывают контроль над аккаунтом жертвы на портале Госуслуги. Это позволяет им осуществлять дальнейшие манипуляции от имени владельца учётной записи, например, оформить займ в микрофинансовой организации. Далее начинается второй этап обмана. Мошенники звонят жертве уже от имени правоохранительных органов или сотрудников Центробанка. Для повышения доверия используются поддельные удостоверения личности, подделывают официальные телефоны и даже предоставляют записи телефонных переговоров. Они запугивают человека, сообщают, что зафиксированы незаконные транзакции или перевод средств в адрес финансирования ВСУ. Для «спасения» всех сбережений необходимо перевести деньги на «специальный счёт «, где они будут храниться до восстановления доступа к аккаунту Госуслуг.

Как защититься:

- Не передавайте никому свои персональные данные, а также коды из сообщений и пароли.
- Проверьте подлинность звонков, позвоните самостоятельно в свою поликлинику или медицинское учреждение по официальному номеру телефона, указанному на сайте учреждения.
- Никогда не отправляйте денежные переводы незнакомцам или лицам, называющим себя представителями госорганов или банковских структур.
- Регулярно проверяйте состояние своего личного кабинета на «Госуслугах», чтобы своевременно выявить попытки несанкционированного входа.
- Используйте двухфакторную аутентификацию везде, где это возможно, включая портал «Госуслуги».

6. Фейковые уведомления от «Почты России».

Злоумышленники рассылают гражданам СМС, электронные письма или сообщения в мессенджерах и социальных сетях, выдавая себя за представителей «Почты России». В уведомлении говорится о якобы поступившем заказном письме из налоговой службы. Для подтверждения получения предлагается перейти по ссылке, которая ведёт на фишинговый сайт или фейкового Telegram-бота, внешне похожие на официальный сервис «Почты России». На этом сайте или в боте пользователю предлагают проверить накладную по номеру трека и подтвердить или отказаться от получения письма. Под предлогом идентификации просят ввести личные данные: ФИО, СНИЛС или ИНН, номер телефона, адрес. Если ввести свои данные на поддельном сайте или в Telegram-боте, то мошенники получат доступ к аккаунту от Госуслуг.

После этого начинается второй этап обмана. Жертве звонит человек, представляющийся сотрудником Росфинмониторинга. Он сообщает, что личные данные попали в руки мошенников, пугает уголовной ответственностью и требует перевести деньги на «безопасный счёт», который на самом деле принадлежит злоумышленникам.

Как защититься:

- Не передавайте никому свои персональные данные, а также коды из сообщений и пароли.
- Проверяйте подлинность звонков: перезванивайте самостоятельно по официальному номеру организации, указанному на её сайте.
- Никогда не отправляйте денежные переводы незнакомцам или лицам, представляющимся сотрудниками государственных органов или банков.
- Заходите в личный кабинет только через специальное приложение или веб-версию официального сайта.
- Отслеживайте заказы только в официальных приложениях или на сайте сервиса.
- Используйте двухфакторную аутентификацию везде, где это возможно, включая портал «Госуслуги».

7. «Подделка рабочих чатов сотрудников организаций».

В последнее время участились случаи мошенничества, при которых злоумышленники используют мессенджеры для создания иллюзии общения внутри организации. Сценарий атаки выглядит следующим образом:

Приглашение в чат

Сотрудник получает приглашение в групповой чат в мессенджере (например, Telegram) с названием, полностью совпадающим с реальным названием его организации, филиала или отдела. Название выглядит достоверно и не вызывает подозрений.

Имитация коллег

В чате находятся аккаунты, выдающие себя за коллег сотрудника, а иногда даже настоящие коллеги, не подозревающие о подмене. Это усиливает доверие к происходящему.

Появление «руководителя»

В чате появляется аккаунт, имитирующий руководителя (директора, завуча, главврача и т. д.), который публикует срочное распоряжение: подтвердить доступ к ресурсу, обновить учётные данные и т. п.

Массовая отправка кодов

Поддельные аккаунты коллег начинают массово отправлять свои коды подтверждения в чат, демонстрируя «исполнительность». Руководитель публично хвалит их за оперативность.

Вовлечение жертвы

Следуя примеру «коллектива», жертва также отправляет свой код, полученный в СМС. На самом деле этот код — авторизационный для входа в её аккаунт на портале «Госуслуги».

Чем это опасно

Получив доступ к аккаунту на портале «Госуслуги», мошенники могут оформлять кредиты в микрофинансовых организациях на имя жертвы; использовать украденные данные для дальнейших попыток хищения денежных средств, в том числе через звонки от фиктивных сотрудников спецслужб; получать доступ к другим персональным данным и использовать их в противоправных целях.

Как защититься

- Не переходите по подозрительным ссылкам и не вводите личную информацию на неизвестных ресурсах.
- Проверяйте подлинность сообщений от официальных организаций через их официальный сайт или горячую линию.

- Не отправляйте коды подтверждения в чаты и не сообщайте их никому, даже если сообщение поступило от «руководителя» или «коллег».
- Не стесняйтесь перезвонить по телефону лично руководителю или тому, от чьего имени запрашиваются данные, чтобы убедиться в достоверности переписки в чате.
- Если сомневаетесь в достоверности информации, обратитесь напрямую в службу поддержки вашей организации или Госуслуг.

8. Фейковое сообщение от «Госуслуг».

Представьте, что вам приходит СМС с сообщением о взломе вашего аккаунта на портале «Госуслуги». В тексте указаны номера телефонов службы поддержки, по которым якобы нужно срочно позвонить, чтобы «спасти» свои деньги и обезопасить аккаунт. Вы звоните, и на другом конце провода — не настоящие специалисты, а мошенники, которые под разными предлогами убеждают вас выполнить их инструкции. Схема может быть многоступенчатой: вас могут переключать между «разными ведомствами» и «государственными организациями», чтобы создать впечатление серьёзности и убедить в необходимости срочных действий.

В результате вы, доверяя «службе поддержки», переводите деньги на «безопасный счёт» или отдаёте их курьеру, тем самым собственноручно передавая их в руки мошенников.

При этом настоящие «Госуслуги» никогда не рассылают такие СМС и не просят звонить по незнакомым номерам. Все официальные уведомления приходят только на электронную почту с адреса no-reply@gosuslugi.ru, а единственный официальный номер техподдержки — 8 800 100-70-10.

Как защититься

- Никогда не звоните по номерам из СМС-сообщений и не переходите по ссылкам в них.
- Проверяйте, действительно ли уведомление пришло с официального адреса.
- Помните, что настоящие службы не просят переводить деньги или устанавливать сторонние приложения.
- Если получили подобное сообщение, лучше самостоятельно зайдите на официальный сайт «Госуслуг» и проверьте состояние аккаунта.
- При подозрительных действиях сразу сообщайте в службу поддержки портала и правоохранительные органы.
- Не поддавайтесь панике. Изучите заранее порядок действий в случае потери доступа к аккаунту Госуслуг.

9. Модератор отзывов на маркетплейсе.

Мошенники продолжают активно использовать схему обмана, предлагая удалённую работу модератором отзывов на маркетплейсах с почасовой оплатой. Эта схема мошенничества нацелена на доверчивых соискателей, особенно тех, кто ищет удалённую работу с гибким графиком. Будьте бдительны и тщательно проверяйте предложения, чтобы не стать жертвой преступников. Для привлечения жертв злоумышленники создают фейковые сайты и распространяют сообщения с заманчивыми условиями — высокой зарплатой, гибким графиком и отсутствием требований к опыту. Чтобы «оформить трудоустройство», у потенциальных работников просят заполнить анкету с личными данными: ФИО, датой рождения, номером телефона, моделью телефона и номером банковской карты. После этого жертве предлагают установить «рабочее» приложение, которое на самом деле является вредоносным ПО. Это приложение позволяет мошенникам получить

полный доступ к устройству пользователя, включая возможность перехватывать коды подтверждения из СМС. Благодаря этому злоумышленники могут войти в личный кабинет онлайн-банка жертвы и удалённо управлять её устройством, проводя финансовые операции без ведома владельца. Данная схема особенно опасна тем, что мошенники не только крадут деньги напрямую, но и могут оформить кредиты на имя жертвы, используя украденные данные. При этом жертвам часто обещают лёгкий и быстрый заработок, что снижает их бдительность. Важно помнить, что настоящие работодатели не требуют предоставления конфиденциальной информации или скачивать программы или приложения из неизвестных источников.

Как защититься

- Никогда не вводите личные и банковские данные на подозрительных сайтах и не переходите по сомнительным ссылкам.
- Не устанавливайте приложения, позволяющие получить доступ к устройству, экрану и управлению по просьбе незнакомых лиц.
- Проверяйте подлинность предложений о работе через официальные сайты и контактные данные компаний.
- При сомнениях обращайтесь в службы поддержки и правоохранительные органы.
- Помните, что настоящие работодатели не требуют оплату за трудоустройство или обучение.

10. «Туристический чат».

Мошенники начали использовать Telegram для создания специальных туристических чатов — небольших тематических сообществ, посвящённых разным странам, курортам и отелям. В этих чатах злоумышленники выдают себя за обычных туристов, которые якобы ищут попутчиков, или за гидов, приглашающих на экскурсии в популярных туристических местах. Такая схема направлена на поиск потенциальных жертв и последующее мошенничество с их деньгами и персональными данными.

Обман заключается в нескольких вариантах действий мошенников:

1. Они могут потребовать предоплату за услуги, например, за экскурсию или организацию поездки, а после получения денег исчезают.
2. Либо предлагают зарегистрироваться на фальшивом сайте, который якобы предназначен для оформления поездки. На этом сайте у жертв запрашивают ввод персональных и платёжных данных, которые затем используются в мошеннических схемах, в том числе для кражи денег.

Как защититься

- Бронируйте туристические услуги только на проверенных и официальных сайтах, а также внимательно читайте отзывы других пользователей, чтобы избежать попадания в ловушку мошенников.
- Будьте внимательны при общении в туристических чатах в Telegram и не переходите по подозрительным ссылкам, не вводите свои личные и платёжные данные на неизвестных сайтах, чтобы не стать жертвой мошенников.
- Если вам предлагают приобрести что-то с большой скидкой — велика вероятность мошенничества.
- Убедитесь, что вы находитесь на официальном сайте туристической компании. С помощью сервиса Whois можно узнать, когда

он зарегистрирован и кто его владелец. Вычислить фишинговый сайт поможет наша инструкция.

- Если у вас возникли малейшие сомнения, не вводите свои личные данные на сайте турагентства, не оплачивайте путёвку онлайн — всё это можно сделать в офисе.
- Никогда не переводите оплату за услуги туристической компании на карту частного лица — если в дальнейшем у вас возникнет спор, то будет очень сложно вернуть свои деньги.