Топ-10 схем мошенников в 2025 году

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?

В 2024 г. мошенники похитили у россиян рекордные [27,5 млрд рублей](https://www.rbc.ru/finances/18/02/2025/67b489749a794780d1527516) с банковских счетов — на 74,4% больше, чем в 2023 г. Основной объём средств (26,9 млрд рублей) был украден у физических лиц. По оценке Сбербанка, ущерб от телефонного мошенничества в 2024 г. составил не менее [295 млрд руб](https://www.rbc.ru/life/news/67c701169a79471c14b76fa5). Согласно опросу Банка России, [34% граждан](https://www.cbr.ru/press/event/?id=23367) сталкивались с различными видами кибермошенничества, при этом 9% из них потеряли деньги.

Мошенники используют разнообразные методы: от телефонных звонков от имени госструктур до фальшивых сайтов и вредоносных приложений. Часто злоумышленники применяют социальную инженерию, запугивая жертв и заставляя их совершать действия, приводящие к потере средств.

Разберём наиболее распространённые схемы мошенничества и способы защиты.

1. Украсть деньги через NFC: «бесконтактный» обман

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 счетов.

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 300 тыс. рублей](https://crimea.ria.ru/20250129/14-letnego-malchika-zastavili-podzhech-zdanie-administratsii-v-moskve-1143766546.html) 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. 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».

4. Мошенники для кражи Telegram-аккаунтов используют игрушки Лабубу

Милашный персонаж зубастый монстр Лабубу стал инструментом в руках злоумышленников, заманивающих детей и взрослых в сети фишинга и иных опасных манипуляций.

Мошенники создают чат-боты в Telegram, обещающие подарок в виде Лабубу за положительный отзыв или участие в розыгрыше. Их цель — привлечь внимание ребёнка или взрослого, заинтересованного популярной игрушкой. Пользователь делится контактной информацией, необходимой якобы для учёта отзыва или подтверждения участия в розыгрыше. После этого поступает сообщение с кодом активации от Telegram. Под видом уникального идентификатора пользователя просят ввести этот код, однако на самом деле этот код открывает доступ к аккаунту жертвы. Получив доступ к учётной записи, мошенники могут использовать её для распространения спама, рекламы сомнительных услуг или даже дальнейших атак на других пользователей.

Кроме того, злоумышленники организуют фальшивые розыгрыши Лабубу, предлагая пользователям подписываться на сторонние каналы в Telegram, в которых рекламируют финансовые пирамиды, нелегальные азартные игры и т. п.

Дети особенно уязвимы перед такими предложениями, ведь они склонны доверять незнакомцам, предлагающим подарки. Родители же редко проверяют безопасность ресурсов, посещаемых детьми, полагаясь на известные бренды игрушек.

Злоумышленники умело маскируют свою деятельность под официальные акции известных брендов, вызывая доверие пользователей. Однако помните: ни один производитель игрушки не попросит вас вводить коды доступа от мессенджеров.

Как защититься:

* Никогда не делитесь личной информацией с неизвестными источниками.
* Будьте осторожны с подозрительными сайтами и группами в социальных сетях.
* Если ваш ребёнок получил предложение поучаствовать в конкурсе или выиграть приз, проверьте надёжность организаторов.
* Настройте двухфакторную аутентификацию для защиты аккаунта Telegram.

5. Подтвердите стипендию на Госуслугах

Телефонные мошенники становятся всё более изобретательными и используют различные методы для кражи личных данных пользователей. Одна из новых схем заключается в следующем — злоумышленники представляются сотрудниками деканатов вузов или архивных служб. В ряде случаев называют конкретные вузы, чтобы вызвать доверие жертвы. Звонящий утверждает, что студенту необходимо подтвердить свою учётную запись на портале Госуслуг, чтобы получить положенную стипендию или продолжить учёбу, сообщает, что необходимо срочно обновить личные данные, иначе их доступ к электронному документообороту будет ограничен. Если студент, озадаченный неожиданно возникшей проблемой, сообщит код из СМС и свои личные данные, то потеряет доступ к своей учётной записи портала Госуслуг.

Затем схема продолжается дальнейшими звонками. Мошенники связываются с жертвой, теперь выступая от имени правоохранительных органов или представителей Центробанка. Они заявляют, что злоумышленники получили доступ к учётной записи Госуслуг после чего произошло хищение денег с карты, и рекомендуют немедленно вывести средства на специальный «безопасный счёт».

Эти звенья мошеннической цепи нацелены на создание паники и заставляют жертву действовать быстро, боясь потерять сбережения. В результате студенты теряют значительные суммы, будучи уверенными, что помогают правоохранительным органам вернуть похищенное имущество.

Как защититься:

* Никогда не передавайте никому пароли и одноразовые коды подтверждения с сайта Госуслуг.
* Настоящие сотрудники университетов не запрашивают такую информацию.
* Регулярно проверяйте историю операций на своём банковском счёте и карте.
* Если замечаете подозрительные транзакции, незамедлительно обращайтесь в банк и блокируйте карту.
* Запрашивайте подтверждение любых действий у официальных контакт-центров учебных заведений и государственных сервисов.

6. Оцифровка пенсий от мошенников

Эта схема, направленная в адрес российских пенсионеров набирает обороты. Злоумышленники создают поддельные групповые чаты в популярных мессенджерах, представляясь сотрудниками Пенсионного фонда России (ПФР). Они распространяют ложную информацию о полном переводе государственной системы обслуживания граждан на цифровой формат. Согласно данной схеме, каждому пенсионеру необходимо пройти обязательную процедуру «оцифровки», включая подтверждение личности на портале Госуслуги и передачу цифровых ключей от Роструда. Это сообщение сопровождается серьёзными предупреждениями — гражданам угрожает приостановка выплаты пенсии в случае игнорирования предложенной процедуры. Для подтверждения своей личности граждане перенаправляются на поддельные (фейковые) страницы, внешне идентичные официальному сайту Госуслуг. Пользователи вводят там свои персональные данные, которые немедленно попадают в руки злоумышленников.

Получив доступ к аккаунтам пользователей портала «Госуслуги», мошенники способны осуществлять следующие противоправные действия:

* Оформление кредитов в микрофинансовых организациях на имя жертвы.
* Использование украденных данных для дальнейших попыток хищений денежных средств, включая звонки от фиктивных сотрудников спецслужб.

Как защититься:

* Никогда не переходите по подозрительным ссылкам и не вводите личную информацию на неизвестных ресурсах.
* Регулярно проверяйте подлинность сообщений от официальных организаций через официальный сайт или горячую линию.
* Если сомневаетесь в достоверности полученной информации, обратитесь непосредственно в службу поддержки пенсионного фонда или Госуслуг.

7. Дополнительный заработок

Представьте себе ситуацию: в вашем мессенджере появляется сообщение от привлекательной девушки, предлагающей познакомиться. Вы соглашаетесь и начинаете общение. Вскоре разговор плавно переходит к работе и дополнительному заработку. Незнакомка делится простым способом заработать деньги — оставить отзыв на маркетплейсе к её товарам.

Вы получаете ссылку на ресурс, который выглядит как личный кабинет маркетплейса. Доверяя своей новой знакомой, вы оставляете первые отзывы. Для повышения доверия мошенница даже переводит вам за работу небольшую сумму денег.

Теперь начинается самое интересное. Вам предлагают перейти на следующий уровень заработка, выполняя новые задания, такие как покупка товаров или оформление премиум-подписки, за эти действия предлагается вознаграждение.

После того, как вы выполните одно из предложенных заданий, ваша новая знакомая исчезает. Связаться с ней больше невозможно, а ваши деньги безвозвратно потеряны.

Как защититься:

* Будьте осторожны, если кто-то предлагает легкий заработок, особенно через мессенджеры.
* Проверяйте ресурсы: перед переходом по ссылке, убедитесь, что она ведёт на официальный сайт маркетплейса.
* Не доверяйте незнакомцам: даже если вам перевели небольшую сумму, это не гарантирует безопасность в дальнейшем.
* Сообщайте о подозрительных действиях: если вы столкнулись с подобной схемой, обязательно сообщите об этом в службу поддержки вашего банка и правоохранительные органы.

8. 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 приложение необходимо, так как через него будут приходить уведомления о статусе отправки/доставки заказных писем. Однако для авторизации в этом сервисе пользователь должен запустить некое мини-приложение. А на самом деле в таком приложении разворачивается 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 мини-приложения 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:

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

9. Авиабилеты по сниженному тарифу

Мошенники имитируют фейковые льготные предложения от крупных компаний. Поступает телефонный звонок якобы от представителей известных российских авиаперевозчиков. Мошенники представляются сотрудниками авиакомпании и сообщают радостную новость: вам предоставляется возможность купить билет по специальной цене или воспользоваться государственной программой субсидирования тарифов. Это предложение звучит крайне привлекательно, особенно если речь идёт о дальних направлениях или дорогостоящих маршрутах. Чтобы подтвердить бронирование, жертве предлагается пройти простую процедуру: отправляется СМС-сообщение с кодом, который якобы необходимо назвать для завершения транзакции. Казалось бы, ничего подозрительного в этом нет, ведь многие сервисы используют такой способ проверки подлинности действий пользователей. Получив заветный код, мошенник быстро переходит к следующему этапу своего плана. Оказывается, предоставленный код нужен вовсе не для оформления билета. Этот код позволяет злоумышленнику войти в ваш личный кабинет портала Госуслуг. Таким образом, преступник получает полный доступ ко всей вашей личной информации, включая паспортные данные, адрес проживания.

Следующим этапом атаки будет шантаж, направленный на то, чтобы человек, испугавшись, перевёл свои денежные средства якобы для спасения на «безопасный счёт».

Как защититься:

* Никогда никому не передавайте коды из СМС — такие сообщения отправляются исключительно для подтверждения операций лично вами, а не третьими лицами.
* Проверьте номер телефона, с которого поступил звонок. Настоящие сотрудники авиалиний связываются только с официальных номеров, указанных на сайте перевозчика.
* Будьте внимательны: официальные представители авиакомпаний никогда не попросят вас сообщить личные данные по телефону или электронной почте.
* Используйте двухфакторную аутентификацию. Даже если кто-то получит ваши учётные данные, дополнительный уровень защиты сможет защитить ваш аккаунт.

10. Оплатите задолженность за газ

Злоумышленники регистрируют Telegram-аккаунты, названия которых похожи на настоящие учётные записи официальных организаций. Например, используются аббревиатуры вроде «Газпром», «Газэнергосеть» или другие известные бренды. Таким образом создаётся впечатление легитимности и доверия среди пользователей. С этих аккаунтов мошенники совершают звонки по поводу плановой проверки и напоминают о «несуществующем» долге за газ, который необходимо оплатить. Для большей убедительности используют профессиональные термины и точные данные вашей квартиры или дома.

Когда человек соглашается оплатить задолженность, мошенник отправляет специальную ссылку, ведущую на сайт-подделку платёжной системы. Там вас попросят ввести личные банковские реквизиты — номер карты, срок её действия и CVV-код. После ввода ваших данных мошенники мгновенно получают возможность совершить транзакцию и украсть ваши средства.

Как защититься:

* Никогда не переходите по предоставленным ссылкам и не вводите там свои личные и платёжные данные.
* Проверьте наличие долга непосредственно на официальном сайте поставщика газа или позвонив на горячую линию компании.
* Если чувствуете угрозу безопасности, заблокируйте подозрительные номера телефонов и сообщите о ситуации службе поддержки вашего банка.

Мир меняется, технологии развиваются, и вместе с ними появляются новые угрозы. Но именно осведомлённость, внимание к деталям и готовность защитить себя делают нас сильнее перед лицом любых попыток обмана. Зная о методах злоумышленников и оставаясь внимательными, мы способны защитить не только себя, но и тех, кто нам дорог.