

Новые схемы мошенничества: как не потерять деньги в 2026 году.

Схема 1. «Сбрось мне свою геолокацию»

Сценарий начинается безобидно: переписка в боте знакомств, пара фото. Далее собеседник предлагает перейти в мессенджер и «запланировать встречу».

После непродолжительной переписки звучит просьба: «Скинь геолокацию какого-нибудь известного места в твоём районе — так проще понять, где нам назначить встречу». Формулировки мягкие, вежливые и доброжелательные — расчёт на то, что собеседник не захочет выглядеть занудой и скинет координаты. Тем более просят и так всем известную точку в городе, а не личный адрес.

Как только геометка отправлена, мошенник переходит к следующему этапу плана. На телефон приходит видеофайл. В ролике человек сообщает, что по указанным координатам могут проводиться незаконные действия. Видео снято так, чтобы создать ощущение реальности происходящего.

Затем поступает звонок якобы от сотрудника спецслужб. Он сообщает, что передача координат важного городского объекта может трактоваться как помощь в организации теракта, и начинает угрожать уголовной ответственностью за отправку геопозиции.

Далее, чтобы «избежать проблем», человеку предлагают «доказать свою лояльность» и «помочь» правоохранительным органам:

- Показать на камеру квартиру
- Открыть банковские приложения — свои и родителей — и перевести либо снять со счёта деньги
- Найти дома наличные и украшения, подготовить их для «изъятия» — и передать курьеру (им оказывается один из мошенников, который играет роль «сотрудника полиции в штатском»)

Никаких взломов банковских приложений и счётов здесь нет — жертва отдаёт деньги и ценности добровольно. Схема держится на психологии: человек верит, что уже совершил что-то опасное, и пытается «исправить» ситуацию через содействие «органам». Времени осмыслить происходящее нет: преступники давят на то, что действовать нужно срочно — иначе будет поздно.

Критический момент в этой ситуации — первая угроза по телефону. Если сразу положить трубку и не продолжать диалог, схема рассыпается. Помните, что настоящие силовики не проводят «оперативные мероприятия» через мессенджер и СМС, не требуют геолокацию и не присылают курьеров за наличными.

Не выполняйте указания неизвестных, кем бы они ни представлялись. Помните: сотрудники правоохранительных органов могут позвонить только для того, чтобы пригласить в подразделение для личной беседы. И уж точно не будут запугивать и угрожать. Блокируйте таких людей и не вступайте с ними в диалог.

Схема 2. Доверенность через Госуслуги и опасный «безопасный» счёт

Вторая схема сложнее и выглядит примерно так. Жертве — обычно это человек пенсионного возраста — звонит неизвестный и представляется следователем. Сухие формулировки и юридические термины, которые он использует, заставляют поверить, что звонок официальный.

Лжеследователь говорит, что в отношении собеседника выявлена утечка персональных данных — и неизвестные уже оформили доверенность для доступа к деньгам на счётах. Эта

доверенность якобы уже «висит» в разделе документов на Госуслугах и ждет подписания через приложение Госключ.

Дальше идет подробная инструкция: жертве предлагают зайти в свой аккаунт на Госуслугах, установить Госключ, найти доверенность в разделе с документами (для «достоверности» на ней размещают логотип какой-нибудь госструктуры) и подписать ее, чтобы якобы перехватить доверенность у мошенников и заблокировать доступ к банковским картам и счетам.

После подписи начинается вторая часть спектакля. Звонит другой псевдосотрудник полиции и заявляет, что первый звонивший был мошенником — и теперь счета действительно в опасности.

Решение, которое предлагают жертве:

- Срочно идти в банк
- Снять все деньги со счетов и передать их «сотруднику в штатском»
- Якобы он временно разместит сумму на «специальном безопасном счете»

Другой вариант — собеседника убеждают самостоятельно перевести деньги на «безопасный счет». Злоумышленник просит никому не рассказывать о его указаниях, чтобы «не помешать оперативным действиям». Благодаря этому у аферистов появляется запас времени, чтобы успеть вывести деньги до того, как подоспеет помощь.

На самом деле доверенность, которая дает доступ к банковским счетам и позволяет распоряжаться деньгами, составляют только очно — в банке или у нотариуса. Через Госключ и любое другое приложение для электронной подписи такая доверенность не оформляется. Многие об этом не знают — и поэтому верят мошенникам.

Помните: ни один документ в Госуслугах не может открыть кому-либо доступ к вашим счетам и деньгам. Мошенники используют электронную «доверенность» как психологический крючок. Деньги жертва передает злоумышленникам самостоятельно: переводом или наличными.

Схема опасна тем, что очень похожа на реалистичный сценарий:

- Мошенники ссылаются на реальный сервис — Госуслуги. Он вызывает доверие. Также они называют реальные факты о человеке: полное имя, дату рождения, адрес прописки.
- «Документ» на Госуслугах действительно есть — злоумышленники подгружают фальшивую доверенность в личный кабинет жертвы. Отправить «доверенность» можно от имени организации или ИП, либо через аккаунт жертвы, украв или подобрав пароль. Чтобы этого не случилось, стоит придумывать сложные пароли, не хранить их в открытом доступе и менять каждые несколько месяцев.
- Если вы увидели доверенность в своем кабинете на Госуслугах, проверьте раздел «Действия в системе» на предмет несанкционированных доступов и смените пароль — подробную инструкцию читайте в нашей [статье](#).

Схема 3. Поддельные службы доставки

В этом сценарии мошенники притворяются специалистами известных служб доставки: СДЭК, Яндекс Доставка, Сбермаркет, Delivery Club. Они пишут людям в мессенджерах с поддельных аккаунтов этих сервисов, которые похожи на реальные: мошенники используют такие же логотипы, описания и названия, стилистику общения.

Люди получают сообщения примерно такого содержания: «Ваш заказ готов к доставке, подтвердите адрес» или «Для выдачи посылки оплатите хранение/доплату за вес». Дальше злоумышленники присылают ссылку «для отслеживания».

Но ссылка ведет не на официальный сайт компании, а на фишинговую копию. На странице предлагают ввести:

- Реквизиты карты
- Логин и пароль от интернет-банка
- Одноразовый код «для подтверждения» операции или входа
- В итоге с карты списывают деньги

Более изощренный вариант схемы — к человеку приезжает реальный курьер с коробкой и QR-кодом для оплаты или подтверждения заказа. Получатель сканирует код, попадает на такой же фальшивый сайт и вводит реквизиты карты, включая секретные данные. Дальше — то же самое: деньги уходят на счет мошенников.

Критичный момент — клик по ссылке. Не стоит открывать ссылки из сообщений или переходить на сайты по отсканированному QR-коду. Вводите адрес сайта нужного сервиса вручную или используйте приложение из официального магазина (например, RuStore, Google Play, Galaxy Store, AppStore). Если человек сам вводит адрес сервисов доставки в браузере или пользуется официальным приложением, шансы наткнуться на клон резко падают.

Схема 4. Маркетплейсы: фейковые блокировки и смена реквизитов продавца

Еще одна рабочая схема — атаки на продавцов маркетплейсов.

Продавцу приходит письмо или сообщение: «Ваш аккаунт заблокирован за нарушение правил. Для продолжения работы подтвердите данные». Внутри — ссылка на «форму проверки», визуально копирующую интерфейс площадки. В действительности это поддельные сайты, как в предыдущей схеме.

Если пользователь вводит логин и пароль, доступ к кабинету уходит злоумышленникам. Дальше возможны несколько вариантов:

- Смена реквизитов для выплат — деньги от реальных заказов начинают уходить на счет мошенников
- Оформление кредитов или рассрочек на продавца под видом «финансирования закупки»
- Кроме того, аккаунт могут использовать для обмана покупателей. Например, разместить выгодное предложение и получать оплату за заказы, не отправляя товар

Маркетплейсы предупреждают партнеров: уведомления о блокировке и проверках приходят либо в личный кабинет продавца либо в официальном приложении. А вот по ссылкам в сообщениях и письмах переходить не стоит.

Схема 5. Лжеинвестиции: поддельные котировки и кража через «комиссии»

Классическая «инвестиционная» схема тоже изменилась. Если раньше мошенники предлагали перевести деньги «в управляющую компанию», то теперь чаще работают через псевдоплатформы.

Человеку звонит «финансовый консультант», ссылаясь на партнерство с банком или крупной компанией и предлагает открыть инвестиционный счет — для старта достаточно небольшой суммы. А чтобы все оформить, нужно перейти по ссылке на сайт, который внешне напоминает известный брокерский сервис.

После пополнения в личном кабинете отображаются вымышленные сделки и растущий баланс. Пока человек наблюдает за «прибылью», все выглядит убедительно. Триггер наступает, когда пользователь решает вывести деньги.

Тогда и появляются дополнительные условия:

- Оплатить комиссию за вывод

- Внести депозит для «подтверждения статуса»
- Оплатить страховку или налоги заранее

Как только перевод отправлен, связь обрывается: мошенники пропадают вместе со всеми деньгами: человек теряет и сумму «инвестиций», и «комиссии».

Правила безопасности те же: чтобы открыть реальный счет у настоящего брокера, регистрируйтесь и проводите операции через официальные приложения и сайты надежных известных сервисов.

Как сохранить деньги в 2026 году: чек-лист

- 1. Прерывайте любой разговор со срочными требованиями.** Если по телефону или в мессенджере торопят, дают, просят действовать «прямо сейчас» — это повод не доверять собеседнику.
- 2. Не переходите по ссылкам из мессенджеров и сообщений.** Доставка, маркетплейс, банк, Госуслуги — чтобы проверить уведомления, открывайте личный кабинет через приложение или вводите адрес официального сайта вручную.
- 3. Ничего не подписывайте в Госуслугах по чьей-то инструкции.** Доверенности, связанные со счетами, оформляют только очно. Если какой-то документ появился без вашего ведома, нужно сменить пароль от личного кабинета — возможно, его взломали.
- 4. Не передавайте данные карты, коды из СМС и доступ к экрану.** Эти данные не нужны ни банку, ни государственным сервисам. Любая просьба показать экран телефона — это повод прекратить любое взаимодействие с собеседником.
- 5. Никому не отдавайте деньги в руки.** Курьеры, «сотрудники спецслужб в штатском», «представители банка», которые приходят за наличными, — это всегда обман.
- 6. Обсуждайте с близкими любые странные ситуации.** Если что-то вызывает сомнения, лучший фильтр — сразу позвонить родным или в свой банк и описать ситуацию. Мошенники всегда просят держать их просьбы в тайне — именно это и должно насторожить.

Главное

Если убрать детали, во всех схемах повторяются одни и те же элементы, а цель мошенников — получить чужие деньги на счет или наличными:

- Собеседника выводят из равновесия — страх, спешка, «уголовная ответственность»
- Человеку показывают что-то визуально знакомое — интерфейс Госуслуг, маркетплейса, доставки
- Мошенники убеждают действовать прямо сейчас и не советоваться с другими

Точка, в которой можно остановить любую схему, всегда одна и та же: тот момент, когда мошенник по телефону или в мессенджере что-то требует — перейти по ссылке, перевести деньги, сообщить данные карты, прислать логины от сервисов, передать наличные третьему лицу.

Помните, что ни один банк, ни один государственный сервис, ни одно ведомство не работает по такому принципу.

Чтобы ваши средства всегда были под контролем и защищены от мошеннических схем, разместите их на вкладе или накопительном счете — отслеживать операции по карте будет удобнее, а ставка обеспечит доходность.