**Памятка для граждан о телефонных мошенничествах**

Телефонное мошенничество известно давно – оно возникло вскоре после массового распространения домашних телефонов. В настоящее время, когда личный номер мобильного телефона может быть у любого члена семьи, от десятилетнего ребёнка до восьмидесятилетнего пенсионера, случаи телефонного мошенничества множатся с каждым годом. В организации телефонных махинаций участвуют несколько преступников. Очень часто в такие группы входят злоумышленники, отбывающие срок в исправительно-трудовых учреждениях. Мошенники разбираются в психологии, и умело используют всю доступную информацию, включая ту, которую жертва мошенничества невольно выдаёт при общении. Чаще всего в сети телефонных мошенников попадаются пожилые люди или доверчивые подростки. При этом каждый человек может стать жертвой мошенничества, если не будет следовать простым правилам безопасности.

**Наиболее распространённые схемы телефонного мошеничества:**

* Обман по телефону: требование выкупа или взятки за освобождение, якобы, из отделения полиции знакомого или родственника.
* SMS-просьба о помощи: требование перевести определённую сумму на указанный номер, используется обращение «мама», «друг», «сынок» и т.п.
* Телефонный номер-«грабитель»: платный номер, за один звонок на который со счёта списывается денежная сумма.
* Выигрыш в лотерее, которую, якобы, проводит радиостанция или оператор связи: вас просят приобрести карты экспресс-оплаты и сообщить коды, либо перевести крупную сумму на свой счёт, а потом ввести специальный код.
* Простой код от оператора связи: предложение услуги или другой выгоды – достаточно ввести код, который на самом деле спишет средства с Вашего счёта.
* Штрафные санкции и угроза отключения номера: якобы, за нарушение договора с оператором Вашей мобильной связи.
* Ошибочный перевод средств: просят вернуть деньги, а потом дополнительно снимают сумму по чеку.
* Услуга, якобы, позволяющая получить доступ к SMS и звонкам другого человека.

**Тактика телефонных мошенников**

Для общения с потенциальной жертвой мошенники используют либо SMS, либо телефонный звонок.

SMS – это мошенничество «вслепую»: такие сообщения рассылаются в большом объёме – в надежде на доверчивого получателя.

Телефонный звонок позволяет манипулировать человеком при разговоре, но при таком общении можно разоблачить мошенника правильным вопросом.

Цель мошенников – заставить Вас передать свои денежные средства «добровольно».

Для этого используются различные схемы мошенничества. Изъятие денежных средств может проходить разными способами. Вас попытаются заставить:

1. Передать деньги из рук в руки или оставить в условленном месте.
2. Приобрести карты экспресс-оплаты и сообщить мошеннику коды карты.
3. Перевести деньги на свой счёт и ввести специальный код.
4. Перевести деньги на указанный счёт.
5. Позвонить на специальный телефонный номер, который окажется платным, и с Вашего счёта будут списаны средства.

**Как правильно реагировать на попытку вовлечения в мошенничество**

Мошенники очень хорошо знают психологию людей. Они используют следующие мотивы:

* Беспокойство за близких и знакомых.
* Беспокойство за свой телефонный номер, счёт в банке или кредитную карту.
* Желание выиграть крупный приз.
* Любопытство – желание получить доступ к SMS и звонкам других людей.

Чтобы противодействовать обману, достаточно знать о существовании мошеннических схем и в каждом случае, когда от Вас будут требовать перевести сумму денег, задавать уточняющие вопросы.

Телефонные мошенники рассчитывают на доверчивых, податливых людей, которые соглашаются с тем, что им говорят, и выполняют чужие указания. Спокойные, уверенные вопросы, отпугнут злоумышленников.

**Что нужно знать, чтобы не стать жертвой телефонных мошенников**

Если Вы сомневаетесь, что звонивший действительно ваш друг или родственник, постарайтесь перезвонить на его мобильный телефон. Если телефон отключен, постарайтесь связаться с его коллегами, друзьями или близкими для уточнения информации.

Помните, что никто не имеет права требовать коды с карт экспресс-оплаты!

Оформление выигрыша никогда не происходит только по телефону или интернету. Если Вас не просят приехать в офис организатора акции с документами – это мошенничество.

Не ленитесь перезванивать своему мобильному оператору для уточнения правил акции, новых тарифов и условий разблокирования, якобы, заблокированного номера.

Для возврата средств, при, якобы, ошибочном переводе существует чек. Не возвращайте деньги – их вернет оператор. Услуга «Узнайте SMS и телефонные переговоры» может оказываться исключительно операторами сотовой связи и в установленном законом порядке.

**Есть несколько простых правил:**

* отметить в телефонной книжке мобильного телефона номера всех родственников, друзей и знакомых;
* не реагировать на SMS без подписи с незнакомых номеров;
* внимательно относиться к звонкам с незнакомых номеров.

## Почему жертву так просто обмануть

Вот порой слушаешь все эти истории и диву даешься: как вообще на такое можно повестись? Очевидно, что это мошенники. А потом удивляешься еще сильнее: жертвой стал не очередной наивный пенсионер, а прогрессивный молодой человек или девушка, которые уж точно должны распознать мошенника.

Дело в том, что телефонные мошенники — отнюдь не «брутфорсеры», которые пытаются отыскать в базе «клиентов» хоть кого-то доверчивого. Они продумывают все до мелочей, строят сценарии разводов по методам социальной инженерии и давят на самые больные места. А еще они чаще всего знают многие персональные данные, включая ФИО, адреса почты, домашний адрес, все банки, где хранятся ваши деньги, марку и госномер машины, имена членов вашей семьи и многое другое. Каким образом эта информация попадает в руки мошенников — отдельная тема, которой касаться в этом материале не будем.

Мошенники прессуют жертву несколькими темами — невероятной срочностью, почти упущенной выгодой, страхом потерять деньги, страхом за близких, страхом раскрытия секретов, страхом получить уголовный срок и другими. Так как мозги всех людей устроены примерно одинаково, то и схемы чаще всего применяются универсальные. И на них ведутся не только пенсионеры, но и молодые люди, считающие, что они-то точно вне угроз.

### Ранее мы рассказывали:

[Заветный CVV: почему опасно привязывать банковские карты к соцсетям](https://blog.eldorado.ru/publications/zavetnyy-cvv-pochemu-opasno-privyazyvat-bankovskie-karty-k-sotssetyam-42371)

## Что такое телефонное мошенничество

В нашем уголовном кодексе нет отдельной статьи для телефонного мошенничества. Оно попадает под общую статью 159 УК РФ. Согласно ей, мошенничество — это хищение чужих средств, имущества или присвоение прав на все это с помощью обмана или злоупотребления доверием.

Конкретно телефонное мошенничество связано не только со звонками. Оно также включает в себя SMS, сообщения в мессенджерах, вредоносные программы с вирусами, общение на сайтах объявлений и многое другое. Видов телефонного мошенничества гораздо больше, чем может показаться на первый взгляд.

Расскажем о пятнадцати актуальных методах развода от телефонных трикстеров. Помните, что на самом деле схем очень много, и понимать, что вас пытаются развести, часто придется интуитивно.

## Виды телефонного мошенничества

### Платный перезвон

Один из старейших способов развода, который существовал еще до появления смартфонов. И ведутся на него ничуть не меньше, чем двадцать лет назад.

Суть в следующем: на ваш телефон поступает звонок с неизвестного номера. Если успели поднять трубку — происходит сброс, а в самых вопиющих случаях перед этим даже можно услышать что-то вроде: «Перезвони срочно на этот номер». Качество связи хромает, личность собеседника определить невозможно. Жертва без задней мысли перезванивает, а звонок оказывается платным — и со счета телефона списываются деньги.

На том конце провода могут даже ответить. С вами будет говорить мошенник, пытаясь удержать вас на линии как можно дольше, пока деньги будут списываться за каждую минуту разговора.

### «Родственник» просит о помощи

Этот способ чаще работает с теми, у кого есть взрослые дети. Родителям звонят с неизвестного номера. Связь плохая и с помехами, голос часто «заикается» и говорит, что это ваш сын или дочь. Мошенник плачет и говорит, что у него случилось что-то очень плохое (попал в аварию, например) и ему срочно нужны деньги на взятку полиции. А если денег не будет, то его вот прямо сейчас закроют на десять лет или даже вывезут в лес и убьют. Спасти бедолагу может только перевод энной суммы на еще один номер.

Это работает, потому что часто мошенники предварительно взламывают телефон жертвы и находят там все данные по его сыну или дочери. Могут даже прослушать их аудиосообщения и повторить голос с помощью специальных программ. Повестись на такое очень легко.

### «Полиция» требует денег

Этот способ часто работает в связке с предыдущим, но может быть и «сольным номером». Вам звонит какой-то «майор» и сообщает, что ваш ребенок совершил страшное преступление. Решить вопросик можно, отправив товарищу майору денег в качестве взятки. В ход идут не только угрозы дать ребенку максимальный срок, но и предупреждение о насилии или даже убийстве.

Иногда «майор» дает пару минут на то, чтобы собрать деньги или взять их у кого-то в долг. Обычно во время этого звонит липовый ребенок, который говорит, что ему конец, а маме или папе нужно поторопиться со сбором денег.

### «Мобильный оператор» грозит блокировкой номера

Относительно свежая схема мошенничества, которая добралась уже до всех операторов связи. Вам якобы звонит ваш оператор и говорит, что у вас либо произошло превышение трафика, либо изменился тариф, либо случился какой-то сбой. В любом случае результат один — номер будет заблокирован, возможно, навсегда. Но без паники — вам нужно лишь совершить некоторые действия и назвать «сотруднику» секретный код из SMS. Если вы высказываете сомнения, то мошенник грозится штрафом.

После оглашения кода из SMS происходит списание либо средств со счета телефона, либо денег с вашей карты — в зависимости от того, какая цель у мошенника.

### Звонок для идентификации от «Госуслуг»

Эта схема давит сразу на несколько болевых точек. Главная из них — страх потерять доступ ко всем функциям «Госуслуг», а заодно сопутствующим сервисам. Мошенник может вам сообщить, что без этой обязательной процедуры вас больше не будут обслуживать в госучреждениях и муниципальных службах, например в поликлинике.

Суть в следующем: вам звонят с незнакомого номера и представляются сотрудником «Госуслуг». Говорят, что надо провести идентификацию личности. Для этого нужно сообщить данные для авторизации и код из SMS. Аккаунт на «Госуслугах» после этого у вас украдут.

Последствия такого развода могут быть самыми разными. Например, мошенник может с помощью вашего аккаунта на «Госуслугах» пройти идентификацию в сервисах спортивных ставок и лотерей. Или оформить на вас микрокредит, деньги от которого, само собой, вы никогда не увидите, а вот отдавать долг придется именно вам.

### «Служба безопасности» банка спешит защитить ваши деньги

Самая распространенная схема развода в России. Вам звонит якобы сотрудник службы безопасности банка и называет вас по имени. Сообщает, что кто-то пытается либо совершить с вашей карты перевод, либо взять на ваше имя кредит. Но не волнуйтесь, все под контролем, вам всего лишь нужно создать заявку на «контркредит» и отправить все ваши деньги на «безопасный счет».

Настоящие банковские работники давно твердят: если вам звонят из банка и говорят о каких-то списаниях, бросьте трубку и перезвоните на официальный телефон горячей линии. Вам ничего за это не будет, как бы ни пытались мошенники убедить вас в обратном.

### Вы выиграли в лотерею!

Если вы когда-нибудь покупали лотерейные билеты и регистрировали их, то ваши данные находятся в системе «Единый ЦУПИС». Иногда каким-то чудом данные о клиентах попадают в неправильные руки, и мошенники могут позвонить, чтобы сказать, что вы стали победителем лотереи. Оказалось, что один из ваших старых билетов содержал в себе победную комбинацию на целую кучу деньжищ. И еще не поздно забрать свой выигрыш.

Но для его получения, конечно же, надо сперва сверить все данные. Вас попросят назвать логин с паролем от банковского приложения и код из SMS для «получения денежного приза». Никаких денег вам никто не даст, даже напротив — заберут себе все, что лежит на карте.

### «Случайно» перевели вам деньги, верните, плиз

Сперва вам приходит SMS, очень похожее на пуш от банка или мобильного оператора. Мол, на ваш счет или номер поступил перевод на относительно небольшую сумму. Это не настоящее оповещение, а «крючок» от мошенников.

Через какое-то время вам поступает либо еще одно SMS, либо звонок с незнакомого номера. Собеседник скажет, что отправил по ошибке деньги не на тот номер или не на ту карту, после чего будет слезно просить отослать их обратно. Добродушные люди подвоха не заметят и захотят сделать, как им кажется, доброе дело — вернуть по ошибке полученные деньги. А на самом деле жертва отдаст рубли из собственного кошелька, ведь никакого перевода на его счет изначально не было.

Оплатите «штраф» со скидкой

Не все владельцы авто знают, что штрафы ГИБДД можно оплатить со скидкой в 50%, если сделать это в течение 20 дней в онлайн-режиме на «Госуслугах». Если к мошеннику попала информация, что вы получили штраф, например, за превышение скорости или разговор по телефону во время вождения, он может позвонить и представиться сотрудником «Госуслуг». Он может сказать, что штраф нужно оплатить прямо сейчас, иначе скидка сгорит, после чего отправит мошенническую ссылку на оплату. Само собой, деньги уйдут не в госструктуру, а на личный кошелек трикстера.

Смотри, какая «фотка»

Кажется, что на этот развод могут попасться только неграмотные в техническом плане пенсионеры, но даже подростков легко ввести в заблуждение таким способом.

SMS в этом случае используются редко, чаще сообщение отправляется в онлайн-мессенджере — WhatsApp, Telegram или аналогичных. Вам со знакомого номера (вашего взломанного знакомого или родственника) приходит файл с названием, которое выглядит примерно как «фотография» или с конкретикой вроде «серега\_чудит\_ржач». Только разрешение у этого «фото» не .png, .jpg или другое, обозначающее изображение, а .apk — это исполняемый файл для Android.

Один раз запустив такой файл, вы подвергаете смартфон заражению. А что будет с гаджетом и вашим банковским счетом потом — зависит только от фантазии и навыков мошенника.

Ранее мы рассказывали:

[Новая угроза: как не лишиться денег из-за трояна](https://blog.eldorado.ru/publications/novaya-ugroza-kak-ne-lishitsya-deneg-iz-za-troyana-42676)

Друг, дай в «долг»

Метод мошенничества, который может превратить вас в законченного технофоба.

Сперва взламывают аккаунт вашего родственника или друга. Трикстер изучает его переписки с вами, анализирует с помощью нейросетей голосовые сообщения и подделывает их. Вам приходит аудио от друга или родственника, которое тяжело отличить от настоящего. В сообщении вас просят дать денег в долг, потому что произошла какая-то неприятная ситуация. Долг вам, конечно, вернут буквально завтра-послезавтра.

Но вместо номера друга или родственника мошенник дает данные третьего лица. На вопрос, почему нужно отправить деньги именно туда, собеседник обязательно придумает правдоподобное объяснение.

### Мошенничество на «Авито»

«Авито» — самая благодатная для мошенничества платформа. Там есть целая тонна схем развода. И все они тоже относятся к категории телефонного мошенничества.

Например, вы хотите купить какой-то товар. Связываетесь с продавцом, а он говорит, что покупателей целая куча и вам надо «забронировать» покупку, выслав предоплату. После отправки денег мошенник, конечно, исчезает.

Или вы сами выставляете лот на продажу. Мошенник пишет, что готов внести предоплату, чтобы точно купить товар. Просит назвать номер карты, срок действия, трехзначный код, затем — цифры подтверждения из SMS. Известен [случай](https://mihadm.com/officially/interesno/page2496), когда житель Пермского края, продавая на «Авито» шкаф, лишился всех своих сбережений — потерял 12 миллионов рублей.

### Вам доступен налоговый вычет

По этой схеме жертве снова звонит липовый сотрудник «Госуслуг» или оператор колл-центра налоговой. Мошенник предлагает по упрощенной схеме и по повышенной ставке оформить налоговый вычет, но, если не сделать этого в рамках звонка, акция закончится. И это очень популярный вариант развода, потому что налоговым вычетом в 2024 году пользуется более 6% населения России.

Дальше все по стандартной схеме: у вас либо попытаются выудить данные авторизации на «Госуслугах», либо запросят всю информацию по банковской карте, включая код из SMS.

### SMS о покупке, которую вы не совершали

Один из вариантов «ленивого» развода. Мошенники массово отправляют тысячам людей SMS с сообщением якобы от банка, где говорится о списании средств за какую-то покупку. А в конце будет фраза: «Если вы не совершали эту покупку, обратитесь по номеру...» — или ссылка якобы на сайт банка, где у вас попытаются украсть учетные данные.

Дальнейшее развитие событий может быть каким угодно. Если вы позвоните по номеру, скорее всего, у вас попробуют выудить данные банковской карты, чтобы списать с нее средства. Хуже, если вы перейдете по ссылке. Мало того, что можете лишиться доступа к аккаунту банка, так еще и подцепите на смартфон вредоносные приложения. И тяжелые последствия не заставят себя долго ждать.

### Вам вменяют «Государственную измену»

«Сбер» еще в прошлом году [раскрыл](https://www.rbc.ru/society/13/03/2023/640ee7c79a794785889ce6fe) новую схему мошенничества. Жертве звонит якобы сотрудник полиции или ФСБ. Он сообщает, что недобросовестный банковский работник крадет деньги со счета жертвы и отправляет их на поддержку ВСУ. Человек, которому поступил такой звонок, в панике, ведь ему вменяется госизмена, а за нее грозит до 20 лет лишения свободы.

В попытке остановить это безобразие жертва переводит на «безопасный» счет свои сбережения и кредитные деньги. Кредит нужно взять якобы для того, чтобы исчерпать лимит займов и не дать сделать это злодею из банка.

### Ранее мы рассказывали:

[Что делать, если сообщил свой пароль от «Госуслуг» другому человеку?](https://blog.eldorado.ru/publications/chto-delat-esli-soobshchil-svoy-parol-ot-gosuslug-drugomu-cheloveku-42505)

## Как противостоять телефонному мошенничеству: важные правила

Противостоять разводу очень просто. Для профилактики телефонного мошенничества достаточно следовать нескольким несложным правилам:

* Незнакомый номер — красный флаг. Впервые видите номер? Не берите трубку и пробейте его в поиске «Яндекса» или Google. Велика вероятность, что этот номер уже известен и зафиксирован как мошеннический.
* Никогда и ни при каких обстоятельствах никому не сообщайте следующую информацию: логины, пароли, PIN-коды, трехзначный код на обратной стороне банковской карты и коды из SMS. Запомните это правило — оно железное. Сотрудники правоохранительных органов, банков, «Госуслуг» и прочих организаций никогда и ни в каких ситуациях не запросят у вас эти данные.
* Включите режим бдительности, если понимаете, что в вас пытаются пробудить какие-нибудь эмоции. Страх за близких, срочность и все в этом духе — красные флаги.
* Найдите способ связаться с собеседником иным способом. Если кто-то просит денег в мессенджере, то позвоните этому человеку по телефону и спросите, действительно ли это делает именно он. Звонят из банка или полиции? Бросьте трубку, найдите актуальный официальный номер в поиске и перезвоните сами.
* Никогда не переходите по ссылкам в SMS или в мессенджерах, если не знаете отправителя. А даже если знаете — трижды проверьте информацию, потому что это может быть скам.
* Вам позвонил незнакомец и затягивает беседу, например, проводя якобы соцопрос? Бросайте трубку — он собирает ваши биометрические данные.
* Вам позвонил явно сгенерированный голос? Смело бросайте трубку — это не обязательно мошенничество, но, вполне вероятно, спам.
* Не поддавайтесь давлению. Мошенники часто создают чувство срочности и критичности. Возьмите паузу и обдумайте ситуацию.
* Обратитесь за помощью к близким, если на вас давят. Вы можете не подозревать, что вас уже опутали сети социальной инженерии. Бдительный супруг или друг помогут трезво оценить ситуацию.