Телефонные мошенники: новые способы обмана в 2023

Как заблокировать навязчивый спам и избежать потери денег?

[Обсудить](https://vc.ru/u/1794325-margarita-maleeva/691301-telefonnye-moshenniki-novye-sposoby-obmana-v-2023?comments)

28 178 просмотров

Думаю, каждый хотя бы раз в жизни сталкивался с телефонными мошенниками и звонками "из банка". Подобные индивиды не стоят на месте, и схем "развода на деньги" с каждым днем становится всё больше, а некоторые из них буквально удивляют своей изощренностью.

Меня зовут Маргарита, я работаю в IT-компании, которая занимается разработкой программы для видеонаблюдения Xeoma и ПО для блокировки спам-звонков KnownCalls. В этой статье мне хотелось бы осветить некоторые виды мошенничества и способы как от них защититься, а также уберечь своих близких, в частности, пожилых родителей и детей. Ведь "Предупрежден — значит вооружен", а для борьбы с мошенниками лучший способ — это рассказать об их методах и пресечь контакт, дабы не попасться на их уловки.

Итак, давайте разберем какие же мошеннические схемы популярны на данный момент:

Звонки из банка

Самый распространенный способ мошенничества, порой поражающий своей абсурдностью. Чаще всего подобные звонки поступают от мошенников, которые представляются "службой безопасности (*название*) банка" и заявляют о подозрительных операциях по карте/счету, а также о заявках на кредит, ипотеку, о смене финансового номера и т. д. На бумаге это звучит неубедительно, но надо понимать, что мошенники не только тонкие психологи, отработавшие каждое предложение и каждый довод на тысячах жертв, но и зачастую обладают вашими персональными данными, которые вы, как вам кажется, нигде не указывали. Это добавляет доверия их словам, ведь у кого, как не у банка, есть доступ к таким данным? К сожалению, персональные данные граждан [утекают](https://www.vedomosti.ru/technology/news/2022/08/29/938017-sdek-podtverdil-fakt-utechki-dannih)как из [государственных источников](https://www.rbc.ru/technology_and_media/11/10/2022/634541439a79470e3efb1ef5), так и из [приложений по доставке](https://journal.tinkoff.ru/news/yandex-food-leak/), а ещё мошенники могут “приобрести” данные о гражданине, который приписан к больнице, пользуется госпорталами и т.п.

Но на дворе 2023 год, и подобные схемы обзавелись новыми инструментами. Одним из новых видов мошенничества можно назвать звонок с просьбой установить на свой телефон специальное ПО "для проверки устройства на фишинговые программы, которые крадут ваши данные". А изюминкой этого метода является просьба зайти в AppStore (или Google Play market) и скачать "приложение для проверки", набрав в строке поиска, скажем, "[Поддержка ВТБ](https://support.google.com/googleplay/thread/200853412/%D0%9F%D1%80%D0%B8-%D0%B7%D0%B0%D0%BF%D1%80%D0%BE%D1%81%D0%B5-%D0%9F%D0%BE%D0%B4%D0%B4%D0%B5%D1%80%D0%B6%D0%BA%D0%B0-%D0%92%D0%A2%D0%91-%D0%BF%D0%BE%D0%BA%D0%B0%D0%B7%D1%8B%D0%B2%D0%B0%D0%B5%D1%82-%D0%BF%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F-%D0%BA%D0%BE%D1%82%D0%BE%D1%80%D1%8B%D0%B5-%D0%B8%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D1%83%D1%8E%D1%82-%D0%BC%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D0%B8%D0%BA%D0%B8?hl=ru)", а там....\*барабанная дробь\*...первым в поиске вы увидите приложение AnyDesk! Это программа для удаленного управления устройством. Т.е. по сути вы устанавливаете на свой телефон программу для удаленного доступа и даёте данные для подключения мошенникам, а они уже в свою очередь крадут все ваши данные и деньги через приложения банков или установив другое ПО, например, для использования криптовалют, абсолютно без вашего участия.

***Что делать:*** в идеале не продолжать разговор, а сразу вешать трубку, т.к. служба безопасности банка давно никому не звонит, да и помимо звонка банк чаще присылает СМС (с официального номера банка, например, 900 у СберБанка) или уведомление в приложении. В приложениях банков настроить двухфакторную аутентификацию (по лицу/пальцу, код-паролю и СМС) для подтверждения каждой транзакции. Если сомневаетесь в чем-то - звоните напрямую в банк, а лучше сходите к ним в офис. В приложении банка вы всегда можете "заблокировать" свою карточку.

Если не уверены, что сможете справиться с давлением профессиональных гипнотизеров, то лучше полностью исключить поступление таких звонков на уровне настроек телефона (где это возможно) или через приложение по блокировке звонков. Также фильтрацию звонков можно настроить у провайдера телефонных услуг (но данная услуга чаще всего платная).

***Что не делать:*** по телефонной просьбе ни в коем случае не устанавливать никакие сторонние приложения, не переходить по ссылкам, НИКОГДА не давать данные своей карты (номер, ФИО, дату и код) и не говорить коды из СМС, не перечислять никуда никакие деньги.

Звонки из полиции, от юристов

Звонки от полиции - это второй по популярности вид мошенничества после звонков из банка. "Вам грозит штраф", "Вас просят явиться", "Вы замешаны в деле..." и тому подобное может выбить из колеи любого, особенно неподготовленного человека, скажем, пенсионера. В этом случае мошенники стараются создать максимально стрессовую атмосферу, говорят громко, быстро и в агрессивном тоне, обвиняя своего собеседника в пособничестве преступлению и угрожая тюрьмой. Но всё всегда заканчивается тем, что звучит сумма, которая может "исправить положение", и предлагаются способы перевода этой суммы. Сейчас очень часто мошенники пользуются криптокошельками, чтобы переводы невозможно было отследить.

***Что делать:*** как и в прошлом пункте, разговор лучше не продолжать, а сразу класть трубку. Если это пугает, то можно сказать "вышлите мне всю информацию письменно на мой адрес", а затем СРАЗУ положить трубку.

Опять же, если вы хотите избежать стресса от подобных провокационных вопросов, вы можете полностью отказаться от звонков с неизвестных номеров, настроив блокировку в приложении по блокировке звонков или, если такая настройка есть, самом телефоне. Ваш мобильный оператор тоже может предлагать такую услугу, так что стоит уточнить у него.

***Что не делать:*** по телефону НИКОГДА никому не давать данные карты, не перечислять деньги и не переходить по ссылкам.

Звонки из пенсионного фонда

Все базы мошенников сейчас содержат не только ФИО обладателя номера, но и другие персональные данные, скажем, дату рождения. Поэтому часто пожилым людям поступают звонки из фальшивого "пенсионного фонда" с просьбой подтвердить списание всех накопленных средств. Мошенническая схема проста: сначала запугать пенсионера, а затем предложить "дать данные своей карты/счета" или же "зайти в приложение и продиктовать...", дабы "заблокировать операцию по списанию средств". Схемы могут различаться, но суть одна и та же, заставить пожилого человека распрощаться со всеми нажитыми деньгами. Иногда данные схемы длятся неделями, "разводя" доверчивого пенсионера на кредит в банке и перевод взятых денег на криптокошелек.

***Что делать:*** сразу класть трубку, а затем звонить в свой пенсионный фонд или идти к ним лично. Пенсионные фонды практически никогда и никому не звонят и уж тем более ничего не предлагают. Настроить блокировку спама на уровне телефона или через приложение по блокировке звонков, также можно настроить фильтрацию звонков у провайдера телефонных услуг (данная услуга чаще всего платная).

***Что не делать:*** истина всё ещё стара как мир — НИКОГДА никому ничего не переводить по телефонной просьбе и не диктовать данные своей карты.

Звонки от "сына, дочери, племянника" и любого другого родственника

"Мама, я попал в аварию" раздаётся в трубке, далее идет протяжный крик, и трубку отбирает представитель полиции или же каких-то других служб. Томным голосом он называет свою ФИО и сообщает о том, что "ваш сын/дочь/реже племянник или внук" попали в серьезную аварию и нуждаются в помощи. Далее начинаются психологические игры с давлением на ответившего со словами "нужно срочно", "прямо сейчас", а потом идут угрозы тюрьмой или тяжким вредом здоровью. Абсурдность ситуации состоит в том, что часто "факты" можно легко проверить, но пожилые люди на эмоциях верят всему, и не задумываясь переводят деньги и отдают данные карт с последними накоплениями, чтобы выручить родственника из беды.

***Что делать:*** подобные беседы сразу же заканчивать и звонить самому родственнику или его знакомым, а также другим представителям семьи. Можно еще погуглить номер местного участкового, если есть какие-то сомнения, и позвонить ему с просьбой проверить обстоятельства. Инструктировать своих пожилых родителей о том, что делать в подобной ситуации и кому из доверенных контактов можно позвонить, чтобы уточнить вопрос. Настроить блокировку спама на уровне телефона или через приложение по блокировке звонков, также можно настроить фильтрацию звонков у провайдера телефонных услуг (данная услуга чаще всего платная).

***Что не делать:*** НИКОГДА никому ничего не переводить по телефонной просьбе и не диктовать данные своей карты.

Звонки из страховой организации

В России страхование жизни или недвижимости не развито так же сильно, как, например, страхование авто, но тем не менее и данные уловки мошенники используют для обмана потенциальных жертв. Чаще всего такие звонки поступают людям преклонного возраста, предлагается страховка за «бесценок» с «очевидной выгодой», а затем вежливым голосом предлагается «сделать всё за вас», и выманиваются данные карты. Что происходит потом, думаю, всем понятно.

***Что делать:*** не продолжать разговор. Если есть сомнения, попросить выслать все условия на электронную почту (её НЕ ДИКТОВАТЬ) и в бумажном виде на адрес (ТОЖЕ НЕ ДИКТОВАТЬ), а затем положить трубку. Если уж это реальная страховая организация, обладающая вашими персональными данными, то и адрес ваш у них тоже будет записан, поэтому диктовать ничего не нужно. Настроить блокировку спама на уровне телефона или через приложение по блокировке звонков, также можно настроить фильтрацию звонков у провайдера телефонных услуг (данная услуга чаще всего платная).

***Что не делать:*** НИКОГДА никому ничего не переводить по телефонной просьбе и не диктовать данные своей карты.

Базовые советы по телефонной безопасности для всех

В основном, в подобных мошеннических схемах страдают самые уязвимые слои населения, а именно пожилые люди. Ими легче манипулировать, особенно если представиться их родственником или представителем власти. В таком случае сложно будет парировать все уловки мошенника и проще всего обезопасить пожилого человека, настроив ему блокировку любых спам-звонков. Это можно сделать как на уровне телефона (инструкцию можно найти в интернете), так и установив приложение по блокировке звонков. Чтобы обезопасить стариков наверняка, лучше всего использовать приложения, которые работают без интернета и разрешают звонки только от проверенных номеров, скажем, из телефонной книги. Ведь, ответив на звонок с незнакомого номера, человек уже попадает в зону риска, потому что многие мошенники бывают тонкими психологами и умеют играть на чувствах ответившего.

На iOS (айфонах) можно [настроить блокировку нежелательных звонков](https://support.apple.com/ru-ru/HT207099) в несколько кликов в настройках телефона. А вот владельцам телефонов на Android повезло меньше: возможность блокировать спам-звонки была доступна в более старых версиях операционной системы, но в современных версиях, к сожалению, недоступна. Еще часто Android-устройства бывают с кастомной оболочкой от производителя (например, очень популярные аппараты от Xiaomi), которая делает недоступными какие-то функции, включая эту, даже на прошлых версиях ядра Android. Поэтому на Android проще всего скачать приложение-блокировщик звонков. Приложение лучше выбирать без доступа в интернет и не собирающее никаких персональных данных.

И ещё немножко информации, только на тему современных технологий. Думаю, многие слышали про биометрию и запись разговорной речи ответившего. Будущее не за горами, а уже здесь, и подтверждение голосом совсем скоро будет массово внедряться. Естественно, мошенники не дремлют и уже вовсю собирают базы данных голосов, которые можно будет использовать в будущем для управления голосовыми командами или уже сейчас совершать звонки родственникам или коллегам с просьбой [перевести деньги](https://habr.com/ru/news/583590/). Полученные данные можно легко моделировать с помощью нейросетей и создавать целые предложения на базе записанных сэмплов голосов. Именно по этой причине так важно пресекать контакт и не вступать с мошенниками в полемику, а сразу класть трубку.

В любом случае любую поступающую информацию по телефону всегда нужно проверять, каким бы «срочным» делом это не казалось. Берегите свой покой, свои нервы и свои сбережения!