**МБУК «Межпоселенческая библиотека»**

**муниципального образования Темрюкский район**

**Методико-библиографический отдел**

**Памятка**

**Темрюк**

**2025**

**Как работают и обманывают людей телефонные мошенники: полный гид по защите**

«Ваша карта заблокирована!», «Родственник в беде!», «Вы выиграли приз!» — знакомо? За каждым таким звонком — отработанный сценарий выманивания денег. Расскажем, как распознать подвох в первые секунды разговора и какие фразы и уловки используют телефонные мошенники.

В последнее время телефонное мошенничество в России достигло беспрецедентных масштабов. По [данным ЦБ РФ](https://cbr.ru/press/event/?id=23382), в 2024 году мошенники украли рекордные 27,5 млрд рублей со счетов россиян — на 74,4% больше, чем в 2023 году. Основная сумма (26,9 млрд) при этом была похищена у физлиц.

**Главные схемы телефонных разводов в 2024-2025 годах**

Злоумышленники используют не только [социальную инженерию](https://hi-tech.mail.ru/review/129116-sotsialnaya-inzheneriya/?utm_partner_id=515), но и [нейросети](https://hi-tech.mail.ru/review/63074-chto-takoe-nejroset/?utm_partner_id=515), поддельные голосовые модели, синтезированные видео (deepfake) и фишинговые платформы, маскирующиеся под сайты банков или Госуслуги. Рассказываем, как аферисты манипулируют сознанием людей ([особенно пенсионеров](https://finance.mail.ru/2025-03-09/top-4-shem-moshennikov-dlya-obmana-pensionerov-65163544/?utm_partner_id=515)), и почему иногда даже технически подкованные люди попадаются на их удочку. Современные мошенники действуют как профессиональные психологи и IT-специалисты. Условно их схемы можно разбить на несколько категорий, о которых рассказываем ниже.

**Финансовые аферы**

**Блокировка карты**. Обычно поступает звонок от «службы безопасности банка» с сообщением о том, что ваша карта взломана (или есть любые другие угрозы для банковского счета). Чтобы спасти деньги, нужно назвать CVV и код из SMS. Или вообще перевести деньги на «безопасный счет». Это самая популярная схема мошенничества.

**Фейковый инвестиционный бот**. Людям предлагают подключиться к «автоматизированной системе» с доходностью 5-10% в день. Жертвам показывают поддельный график роста депозита, а после внесения денег по надуманной причине блокируют аккаунт, разумеется, вместе с вложенными средствами.

**Мошенничество с рефинансированием кредитов**. «Сотрудник банка» предлагает снизить ставку по текущему кредиту, но для этого нужно оплатить «комиссию за перерасчет». Разумеется, оплата пойдет на счет злоумышленников.

**Манипуляция страхом**

**«Родственник в беде» + дипфейки**. Мошенники используют нейросети для клонирования голоса близких. Затем они давят на больное — сообщают, что ваш родственник попал в беду. Это может быть ДТП (как виновник, так и пострадавший), какая-то травма, срочная госпитализация и другие пугающие сообщения.

**Звонок от имени правоохранительных органов**. Мошенники представляются сотрудниками ФСБ, полиции или прокуратуры и утверждают, что жертва подозревается в госизмене, финансировании терроризма или других тяжких преступлениях. Для «закрытия дела» они требуют перевести деньги на «безопасный счет» или передать данные банковской карты. Для усиления страха и уровня давления аферисты используют актуальные новостные поводы, например, санкции или военные действия.

**Госуслуги и правоохранители**

**«Налоговые долги» с угрозами ареста**. На телефон жертвы приходит SMS с требованием оплатить «просроченный налог» через фишинговый сайт-клон Госуслуг. Далее все данные утекают злоумышленникам.

**«Уголовное дело» по поддельному постановлению**. Мошенники могут прислать фотографию «постановления суда» с вашими данными и потребовать деньги «для прекращения дела».

**Фейковые штрафы ГИБДД с видео**. Здесь работает принцип [фишинга](https://hi-tech.mail.ru/review/121594-fishing/?utm_partner_id=515) — в SMS встроена ссылка на поддельный сайт с видео «вашего нарушения». Чтобы его посмотреть, нужно ввести свои данные или авторизоваться через Госуслуги.

**Технологические ловушки**

**Мошенники звонят под видом службы безопасности банка** и сообщают, что в текущей версии условного Сбера найдена критическая уязвимость. Чтобы ее устранить, нужно максимально оперативно установить новую версию приложения. Далее аферисты присылают вредоносный APK-файл, в котором скрывается [троян](https://hi-tech.mail.ru/review/129077-troyan/?utm_partner_id=515).

**Вирус через QR-код**. В сообщении от «курьерской службы» предлагают отсканировать QR-код для отслеживания посылки. Чтобы заинтересовать человека, часто указывается большая объявленная ценность. QR-код же ведет на сайт с [вредоносным ПО](https://hi-tech.mail.ru/review/129033-vredonosnoe-po/?utm_partner_id=515).

Аферисты под предлогом помощи или решения какой-то проблемы подключаются к устройству через AnyDesk (или TeamViewer) для дальнейшей кражи данных.

**Психологические приемы: 7 уровней манипуляции**

Далее расскажем именно про психологические уловки аферистов, которые хорошо понимают страхи простых людей и умеют на них играть.

**1. Предатака и сбор информации** - мошенники заранее изучают соцсети и слитую информацию о жертве, чтобы упомянуть реальные события. Они могут поинтересоваться, как прошел недавний отдых, или почему вы сменили работу.

**2**. **Создание авторитета** - например, отправка поддельных удостоверений ФСБ с фото и печатями и фоновые звуки «полицейского участка» (звук раций и сирены). Также аферисты стараются «правильно ставить» речь, чтобы она звучала официально и уверенно.

**3**. **Изоляция жертвы** - указание «никому не звонить и не писать, иначе преступники узнают». Очень коварный метод, который оставляет жертву «один на один» с опытными мошенниками и исключают вероятность того, что близкий человек с холодной головой распознает обман.

**4. Двойная игра -** например, «сотрудник банка» сначала помогает отменить несанкционированный платеж, а затем предлагает защитить счет переводом на якобы безопасный аккаунт.

**5. Подмена реальности** - мошенники часто создают копии и клоны сайтов настоящих банков. Они могут использовать их как для фишинга данных, так и для публикации фейковых новостей о взломе банка или глобальной утечке данных.

**6. Симуляция поддержки** - «Я понимаю, как вам страшно. Давайте вместе решим проблему», — так злоумышленники формируют ложное доверие. Они также могут оперировать терминами «Не переживайте, мы прямо сейчас решим вашу проблему» и подобными сообщениям.

**7. Когнитивная перегрузка -** одновременные требования в стиле «Диктуйте код из SMS», «Зайдите на сайт», «Подтвердите данные паспорта» буквально не дают потенциальной жертве трезво подумать и оценить ситуацию. Психологически неустойчивые люди начинают теряться, а в дальнейшем бездумно выполняют команды мошенников.

**Главные признаки телефонных мошенников**

Телефонные мошенники используют человеческие слабости: доверчивость, страх, жадность. Чтобы не стать очередной жертвой злоумышленников, нужно уметь отличать их по очевидным и косвенным признакам.

**Давление и спешка -** мошенники стремятся вызвать панику, чтобы человек действовал необдуманно. Часто поступают угрозы:

- «Ваши деньги будут списаны через 10 минут».

- «Если не переведете деньги, у вашего сына будут проблемы с законом».

- «Это проблему можно решить сейчас, потом будет поздно».

**Запрос конфиденциальных данных** - ни банки, ни государственные органы никогда не запрашивают в телефонном режиме:

- Пароли, PIN-коды, CVV/CVC карты.

- Полные реквизиты карт или паспортные данные.

- Коды из SMS.

**Требование перевести деньги необычным способом** - главная цель злоумышленников — ваши деньги. И часто они просят перевести их странным образом:

- Криптовалюты. Bitcoin и другие анонимные платежи невозможно отследить.

- Электронные кошельки. Переводы на WebMoney или ЮMoney — явный признак аферистов.

**Подозрительный номер звонящего** - мошенники часто звонят со странных и непривычных номеров, чтобы еще больше запутать будущих жертв:

- Международные префиксы, например, +44 (Великобритания) или +1 (США).

- Короткие номера (+1000, 9999 или что-то похожее).

- Городские номера телефонов с кодами из других регионов, например, +7 (343).

**Установите приложение для определения спам-звонков. Они помогут еще до принятия вызова отсеять большинство нежелательных звонков.**

**Технические уловки** - подмена номера. Звонок якобы из банка, но номер не совпадает с официальным. Это может быть номер 90О, где последний символ — это буква «О», а не ноль.

Фейковые SMS. В них присылают ссылки на фишинговые сайты, имитирующие Госуслуги или банки.

**Голосовые сигналы** - обращайте внимание на голосовые факторы:

- Шум, посторонние разговоры, звук клавиатуры и других звонков — частый признак недобросовестного колл-центра.

- Скрипты. Звонящий читает текст, не отклоняясь от сценария, и медленно реагирует на встречные вопросы.

**Чего нельзя делать: 10 фатальных ошибок**

Даже невинные действия во время разговора могут привести к краже данных. Нужно внимательно изучить наши советы, запомнить их и обязательно применять в реальной жизни.

**Итак, чего ни в коем случае нельзя говорить и делать в телефонном разговоре с неизвестными людьми.**

1. Переводить куда-то деньги. Ни под каким предлогом!
2. Диктовать коды из SMS (даже если звонящий знает ваше ФИО, ИНН, адрес и другие данные).
3. Сообщать любую личную информацию и данные о родственниках (имена, контакты, места работы и прочее).
4. Сообщать, что вы одни дома (аферисты поймут, что можно давить на жертву).
5. Называть остаток средств на ваших счетах и картах. Если там большие суммы, злоумышленники просто так не отстанут.
6. Переходить по ссылкам из сообщений, даже если они ведут на «официальный сайт».
7. Устанавливать какие-либо приложения по инструкции звонящего.
8. Отправлять фотодокументов для «проверки личности».
9. Верить в «секретные операции» — настоящие банкиры никогда не просят сохранять разговор в тайне.
10. Использовать публичный Wi-Fi для операций с банком и финансами.

**Мнение экспертов**

Для такой социально-важной темы мы взяли комментарии у двух экспертов. Начнем с Андрея Бийчука, директора продукта «Защитник» МТС.

***Какие виды телефонного мошенничества сейчас самые популярные?***

По нашим последним данным, наибольшую активность проявляют следующие мошеннические схемы:

- 25% — предложения о дополнительном заработке с помощью инвестиционных проектов.

- 20% — звонки под видом представителей банков.

- 18% — звонки от имени мобильных операторов с просьбами срочно продлить номер.

- 9% — обращения от имени сотрудников компаний энергоснабжения и проверки счетчиков.

***Откуда телефонные мошенники знают номера и ФИО людей?***

Мошенники получают информацию благодаря утечкам данных из кредитных организаций, интернет-магазинов и других источников. Данные обрабатываются и объединяются в обширные базы, формируя профили пользователей. В нашем сервисе «Защитник» есть функция поиска утечек персональных данных. С ее помощью пользователи могут узнать о данных, которые утекли, и получить рекомендации о том, как необходимо действовать для сохранности данных.

***Как не стать жертвой обмана?***

Чтобы защитить себя, рекомендуем:

- Завершить разговор и самостоятельно перезвонить по официальному номеру компании, от лица которой исходил звонок.

- Создавать уникальные и сложные пароли для каждого аккаунта, комбинируя буквы, цифры и специальные символы.

- Не раскрывать свои личные данные (например, пароль или номер карты) третьим лицам. Настоящие сотрудники не запрашивают подобную информацию.

- Не переходить по сторонним ссылкам, присланным в SMS.

Валентин Поляков, владелец продукта антивирус в компании PRO32**,**также ответил на наши вопросы о мошенниках.

***Какие технические уловки часто используют телефонные мошенники?***

В качестве примера самых распространенных типов троянов, которые используют телефонные мошенники, можно привести:

Поддельные копии известных приложений, к примеру мессенджера WhatsApp. Сценарий из реальной жизни — пользователь обнаружил, что поддержка мессенджера на его старом смартфоне прекращена, приложение больше не запускается. В поисках решения он нашел телеграмм-канал, в котором был размещен установочный APK-файл WhatsApp для старых версий Android (в данном случае речь шла про Android 4.2). После установки приложение предоставляет злоумышленникам контактные данные пользователя и получает доступ к данным входящих смс-сообщений.

- Пользователь отвечает на звонок, в ходе которого злоумышленники могут обманным путем уточнить дополнительные недостающие сведения. Например, это может быть ФИО или номер паспорта, которые потом используются для оформления микрокредитов и покупок в рассрочку на различных маркетплейсах.

В качестве защиты от такого вида мошенничества рекомендуем устанавливать приложения только из официальных источников (Google Play, RuStore или официальный сайт разработчика, если приложение отсутствует в магазинах приложений). Если ни одна из опций не подходит — в крайнем случае можно воспользоваться тематическими техническими форумами, например, 4PDA, где есть хотя бы минимальная модерация контента.

Во-вторых, всем пользователям устройств на базе Android крайне важно использовать полноценный антивирус для защиты мобильных устройств, так как для Android на сегодняшний день существует огромное количество вредоносного ПО.

В-третьих, не будет лишним установить самозапрет на получение кредитов через Госуслуги, если в ближайшее время вы не планируете их оформление.

Еще один пример трояна, который могут использовать злоумышленники, — это приложения, которые предоставляют полный удаленный доступ к устройству жертвы. Здесь можно выделить два основных сценария — когда пользователь по ошибке самостоятельно скачивает поддельный и пропатченный на предоставление постоянного доступа мошенникам APK-файл приложения, либо когда злоумышленники в ходе телефонного звонка обманом побуждают самого пользователя скачать и установить легальное ПО для удаленного доступа, а он по собственной воле разрешает доступ к устройству.

***Чего ждать от телефонных мошенников в 2025 году?***

- Использование ИИ. Искусственный интеллект обучается, чтобы правдоподобно подделывать голоса и визуальные образы. Это открывает новые возможности для мошенников. Самый простой вариант — это изменение голоса на чужой голос близкого человека на основе заранее полученного образца. Встречаются случаи использования дипфейк-видеозвонков, когда злоумышленник выглядит на видео как знакомый вам человек за счет ИИ-обработки в режиме реального времени. Каждый год качество видеообработчиков только возрастает, и жертвам мошенников становится все сложнее отследить подмену.

- Многоходовки. Мошенники совершают поочередно два звонка. В ходе первого «подозрительного» звонка пытаются выудить у пользователя персональные данные или шантажируют тем или иным способом. Через некоторое время жертва получает второй звонок уже от лица якобы правоохранителей, которые заявляют, что пресекли попытку мошенничества, а для сохранности скомпрометированных данных просят назвать еще больше персональных данных.

- Запугивание «острыми» темами. Очень распространена в последнее время схема шантажа, где жертву якобы уличают в финансировании терроризма, просмотре незаконного в РФ контента и так далее. Зачастую человек впадает в ужас от таких обвинений и в состоянии паники соглашается на любые требования злоумышленников, в том числе оставить «под залог» денежные средства.

**Итоги**

**Будьте бдительны и не доверяйте посторонним людям. Пользуйтесь правилом 10 минут — прервите разговор, посоветуйтесь с близкими и проверьте информацию через официальные каналы.**

**Источник:**

**Как работают и обманывают людей телефонные мошенники: полный гид по защите**. - Текст : электронный. - URL : <https://hi-tech.mail.ru/review/129245-kak-rabotayut-i-obmanyvayut-lyudej-telefonnye-moshenniki/?utm_partner_id=515#anchor17507727538221468> (дата обращения: 08.08.2025)