

1. Что делать, если учетная запись заблокирована или вас взломали?

Если ваша учетная запись заблокирована или вас взломали, то вы можете самостоятельно восстановить доступ, нажав на экране входа кнопку **«Восстановить доступ»**, система автоматически перенаправит вас на страницу восстановления профиля.

Введите номер телефона, который привязан к вашему профилю MAX, а затем нажмите **«Восстановить»** и дождитесь завершения проверки.

Для восстановления профиля используйте браузер **Safari, Google Chrome** или **Яндекс Браузер**.

Обратите внимание: в настройках браузера должны быть разрешены переадресация и всплывающие окна:

- **Safari:**

<https://support.apple.com/guide/safari/ibrwe2159f50/mac>

- **Google Chrome:**

<https://support.google.com/chrome/answer/95472?hl=ru&co=GENIE.Platform%3DAndroid&oco=1>

- **Яндекс Браузер:**

<https://yandex.ru/support/browser/ru/security/permissions>

Чтобы сама проверка прошла корректно, проверьте:

- отключён VPN и Wi-Fi на телефоне;
- включён мобильный интернет;
- убедитесь, что интернет работает именно через сим-карту, к номеру которой привязан профиль MAX;
- если у вас две сим-карты, выберите нужную в настройках телефона или временно оставьте только её активной.

Если ваша учетная запись заблокирована или вас взломали, то вы также можете обратиться в службу **Технической поддержки** по адресу <https://help.max.ru> и описать вашу проблему. Специалисты Поддержки постараются вам помочь как можно быстрее.

В рамках обращения нужно указать:

- номер телефона, на который зарегистрирован ваш аккаунт
- дату и время, когда обнаружили блокировку/взлом
- какие действия выполнялись перед блокировкой/взломом (например, включали VPN, входили с нового устройства, посещали новые ресурсы и т.п.)
- использовали ли вы сторонние клиенты или модифицированные приложения

Важно! Не отправляйте повторные вопросы каждые несколько часов – это увеличивает нагрузку на систему и увеличивает время ожидания ответа на ваш вопрос.

2. Дополнительные рекомендации по безопасности

Пока вы ожидаете ответа Поддержки, рекомендуем выполнить дополнительные действия:

1. Проверить устройство на безопасность

- Рекомендуем просканировать телефон или компьютер антивирусным приложением.
- Убедитесь, что на устройстве нет вредоносных программ, автокликеров или подозрительных приложений.
- Удалите сторонние или модифицированные версии мессенджера (если использовались).

- Обновите операционную систему до актуальной версии (особенно обновления безопасности).

2. Проверить сетевую безопасность

- Отключите VPN, прокси и анонимайзеры.
- Избегайте публичных Wi-Fi сетей без защиты.
- Убедитесь, что SIM-карта зарегистрирована на вас и не перевыпускалась без вашего ведома.

Если устройство окажется заражённым, это может быть причиной подозрительной активности или взлома.

Сразу после разблокировки/возврата аккаунта рекомендуем:

1. Включите двухфакторную защиту (2FA)

(через 24 часа после разблокировки)

Добавьте дополнительный пароль для входа.

2. Привяжите электронную почту

Подтвердите актуальный e-mail для восстановления доступа.

3. Проверьте активные сессии

Завершите все незнакомые сессии.

4. Соблюдайте цифровую гигиену

- Не передавайте коды подтверждения
- Не устанавливайте приложения с подозрительных источников
- Не устанавливайте модифицированные версии
- Не передавайте аккаунт третьим лицам

3. Предостережение о мошенниках

Злоумышленники могут выдавать себя за знакомых, сотрудников банков, сотрудников правоохранительных и государственных органов, поддержку или представителей компаний. Их цель — получить ваши деньги, коды или доступ к аккаунту.

Если вы уже столкнулись с мошенником:

- Немедленно прекратите переписку/звонок.
- Не отправляйте дополнительные данные или деньги незнакомым.
- Сообщите о нарушении через жалобу.