

# Recluse

## User Guide

The private messenger for Android and Windows

Version 0.2.3 · Released 10 November 2026

Download: get.freedomwithrahi.trade

---

*Written for everyday users. You don't need to know anything about computers or security to follow it.*

# What’s in this guide


1. What is Recluse? ..... 3
2. Install Recluse ..... 3
3. First start ..... 6
4. Add a contact ..... 9
5. Chatting ..... 12
6. Groups ..... 15
7. Disappearing messages and privacy options ..... 16
8. Settings, page by page ..... 18
9. Connection and bridges ..... 19
10. Notifications on Android ..... 22
11. Updates ..... 23
12. Problems and how to fix them ..... 24
13. Feedback and help ..... 25
14. Staying safe ..... 26
15. Glossary ..... 27


### How to read this guide

- Words in **bold**, like **New chat**, are exactly what you see on the screen.
- Numbered steps are done in order. Pictures of the screen are next to the steps.
- **Tip** boxes give helpful extras. **Important** boxes warn you about something you could lose or get wrong.
- The pictures come from a test copy of Recluse. Names such as Alice and Bob are examples, and small details, such as version numbers, may look different on your device.

# 1. What is Recluse?

Recluse is a messaging app, a bit like WhatsApp. You can send messages, photos, voice notes and files, and chat in groups. The difference is that Recluse is built for privacy first.

| | WhatsApp | Recluse |
|---|---|---|
| **How you sign up** | With your phone number. | With nothing. You choose a name and a passphrase. |
| **How you add people** | From the contacts in your phone. | With a one-time invite: a QR code or a link. |
| **How messages travel** | Over the normal internet. | Only through Tor, which hides where you are. |
| **Backups and other devices** | Chat backups and linked devices. | No backups and no syncing. Each device is separate. |

### Three words you will see often

- **End-to-end encrypted.** Your message is locked on your device and only unlocked on the other person's device. Nobody in between can read it: not your internet company, not the Recluse server, not anyone else.
- **Tor.** Tor is a free network run by volunteers around the world. Your messages pass through several Tor computers, so nobody can easily see where they come from or where they go. Your internet company can see that you use Tor, but not who you talk to.
- **Passphrase.** A passphrase is like a password, but longer: a few words together. It locks everything Recluse keeps on your device.

### What you need

- An Android phone with **Android 8** or newer, or a Windows PC with **Windows 10 or 11** (64-bit).
- An internet connection (mobile data or Wi-Fi).
- Recluse is not available for iPhone, iPad, Mac or Linux yet.

> **Important:** Recluse is new software. It has not had an independent security audit yet. (An audit is a careful check by outside experts.) It uses well-known encryption, but treat it as new.

# 2. Install Recluse

Recluse is not in the Google Play Store or the Microsoft Store. You download it from its own website: **get.freedomwithrahi.trade**. Type this address into your browser yourself.

> **Tip:** Don't install Recluse from files that people forward to you, for example in WhatsApp groups. A forwarded file could be a fake. Always download it from the website.

## On an Android phone

The Android app is an **APK** file (an Android app file you install yourself). The file is called recluse-0.2.3-release.apk and is about 24 MB.

1. Open your phone's browser, for example Chrome, and go to **get.freedomwithrahi.trade**.
2. Tap **Download**. If your browser warns about the file, tap **Download anyway**.
3. Open the file from the notification, or open **Files**, then **Downloads**, and tap the file.
4. If Android asks, allow your browser to install apps: tap **Settings**, turn on **Allow from this source**, then go back.
5. Tap **Install**. If Play Protect warns about an unknown app, tap **More details**, then **Install anyway**.
6. Open Recluse from your list of apps.

Afterwards you can turn **Allow from this source** off again.

## On a Windows PC

For Windows there are two versions. Both are the same app; they only differ in how they are kept on your PC.

| | Installer | Portable |
|---|---|---|
| **Best for** | Your own PC. | A USB stick, or a PC where you can't install programs. |
| **How it runs** | Installs for your Windows account, with Start menu and desktop shortcuts. No administrator rights needed. | Runs straight from the file. Nothing is installed. |
| **Where your chats are kept** | On the PC, in your Windows account. | In a **Recluse Data** folder next to the file. |
| **Updates** | Downloaded and installed from inside Recluse. | Downloaded for you, but you start the new file yourself. |
| **File (about 106 MB)** | Recluse-Setup-0.2.3-x64.exe | Recluse-Portable-0.2.3-x64.exe |

### Install it

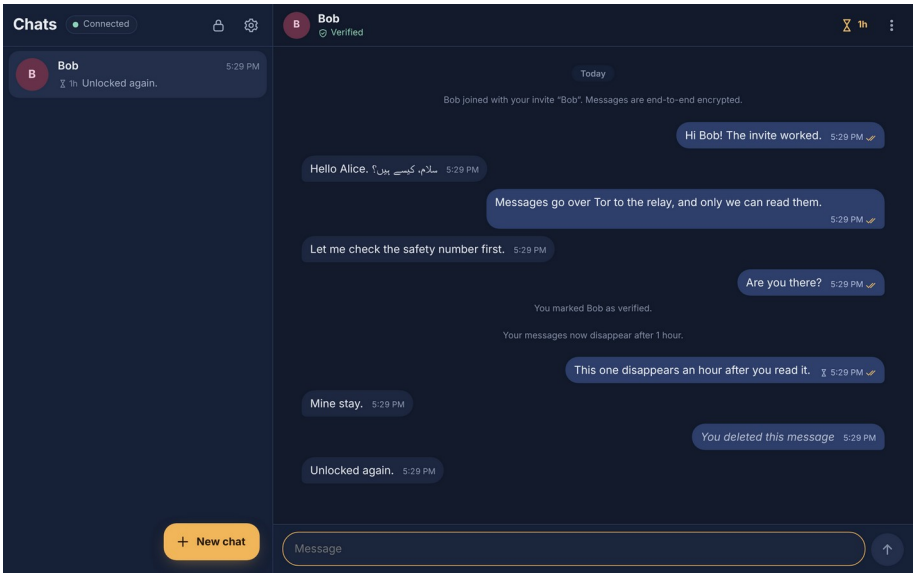
1. Go to **get.freedomwithrahi.trade** and click **Download for Windows**. For the portable version, click **Portable version, no install**.
2. Your browser may warn that the file is unknown. Choose to keep the file. (If you want, check the file first: see "Check your download" below.)
3. Open the downloaded file.
4. Windows may show a blue box: **Windows protected your PC**. This is Windows SmartScreen. It appears because the Recluse files are not "code-signed" yet (code signing is a paid digital stamp). Click **More info**, then **Run anyway**.
5. Installer: follow the steps. You can keep the folder it suggests. At the end, click **Finish** and Recluse starts. Portable: Recluse starts straight away.

**Important:** For the **portable** version:

- Put the .exe file in its own folder first, for example on your USB stick. Recluse creates a **Recluse Data** folder next to it. Keep the file and the folder together. The folder holds your locked chats and keys.
- Use only one copy. Don't copy the Recluse Data folder and use both copies (for example one on the PC and one on the USB stick). Both copies would collect the same messages, and messages can get lost.
- Quit Recluse (see below) before you unplug the USB stick.

### Recluse keeps running in the tray

When you close the Recluse window, Recluse keeps running in the background, so messages can still arrive, and it **locks** itself. You find it in the tray: the small icons next to the clock. Click the Recluse icon to open it again, then unlock. To close it completely, right-click the icon and choose **Quit Recluse**.




*Recluse on Windows: your chats on the left, the open chat on the right.*

## Check your download (optional)

This step is for careful users. It takes about a minute. A **checksum** is like a fingerprint of a file. If the fingerprint of your file matches the one on the website, nobody changed the file on the way.

### On Windows

1. Open **get.freedomwithrahi.trade/verify** in your browser. (Later, inside Recluse, you find it under **Settings**, **About**, **Verify a download**.)
2. Open the folder with the file you downloaded, usually **Downloads**.
3. Click the address bar at the top of the folder window, type **powershell** and press Enter. A PowerShell window opens in that folder.
4. On the verify page, copy the PowerShell command for your file. Paste it into the PowerShell window (right-click pastes) and press Enter.
5. If it prints **True**, the file is genuine. If it prints **False**, or says the file can't be found, check the file name. Still **False**? Don't open the file.

**The Android app:** copy the APK to a Windows PC and check it the same way. Once Recluse is installed, Android itself refuses any update that is not signed with the same key.

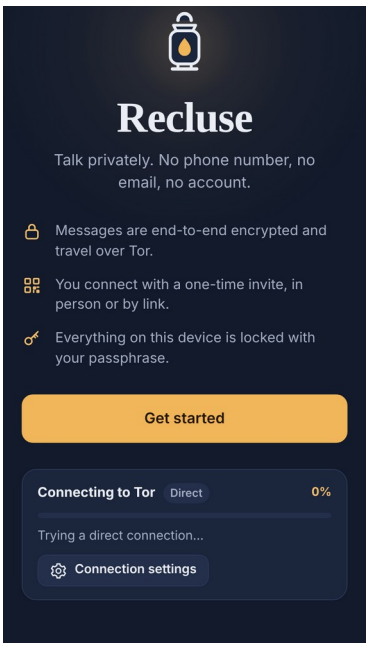
> **Important:** If something doesn't match:
>
> - Don't open or install the file. Delete it.
> - Type **get.freedomwithrahi.trade** into the address bar yourself and download the file again.
> - If it still doesn't match, don't use it until a new version is published.

# 3. First start

## Connecting to Tor

When you open Recluse, it first connects to Tor. You see a box called **Connecting to Tor** with a percentage.

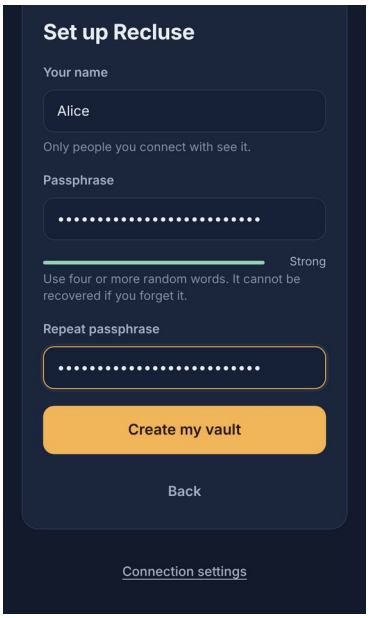
- This often takes under a minute. On slow or restricted networks it can take several minutes.
- You don't have to wait. You can set up your profile while it connects.
- On some networks, including some in Pakistan, Tor is blocked and the progress stops at around 5–10%. If nothing changes for a minute, Recluse says: "Your network may be blocking Tor." In **Automatic** mode it then tries **bridges** by itself. A bridge is a hidden entrance to Tor (see chapter 9). Just give it a few more minutes.




*The welcome screen while Tor connects.*

## Create your profile

1. Tap **Get started**.
2. **Your name:** type the name you want people to see. Only people you connect with see it. You can change it later.
3. **Passphrase:** type your passphrase (see the advice below). A bar shows how strong it is: Too short, Weak, Good or Strong. Use at least 8 characters.
4. **Repeat passphrase:** type it again.
5. Tap **Create my vault**. Your **vault** is the locked storage on your device that holds your chats and keys.
6. Wait a moment while it says **Creating your vault**. This is slow on purpose: it makes your passphrase very slow to guess.
7. You now see **Chats**. You are ready to add your first contact (chapter 4).




*Set up Recluse.*

## Your passphrase

> **Important: there is no “forgot password” email**
>
> Nobody can recover your passphrase. Not us, and not anyone else. Recluse never stores it and never sends it anywhere.
>
> If you forget it, the chats on this device cannot be opened. You would have to delete everything and start again, and your contacts would need a new invite from you. So please take a minute now to choose it well and keep it safe.

### How to choose a strong passphrase

- Use **four or more random words**, for example “mango kettle river seven”. (Don’t use this example. Make your own.)
- The words can be English, Urdu written in English letters, or any language you know well.
- Don’t use your name, birthday, phone number, or a famous line from a song or poem.
- Don’t use a passphrase you already use for another app or for email.
- Longer is stronger.

### How to keep it safe

- Practise typing it a few times on the first day.
- If you write it down, keep the paper in a safe place at home, away from your phone. Don’t save it as a photo or a note on the same phone.
- Don’t tell it to anyone. Recluse only ever asks for it inside the app.
- If you think someone saw it, change it: **Settings**, **Security**, **Change passphrase**.

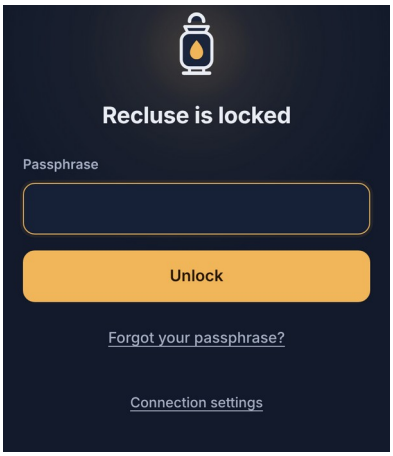
## Locking and unlocking

Recluse locks itself after 5 minutes without use. You can change this in **Settings**, **Security**, **Lock automatically**.

To unlock, type your passphrase and tap **Unlock**.

To lock Recluse yourself, tap the **padlock** icon at the top of the chat list. Your chats stay hidden until you unlock.

Recluse also locks when you **close** it: on Android when you swipe it away in the list of recent apps or press **Back** on the chat list, on Windows when you close its window. Messages keep arriving while it is locked. Pressing **Home** or switching to another app doesn't lock it straight away: the **Lock automatically** timer does that.



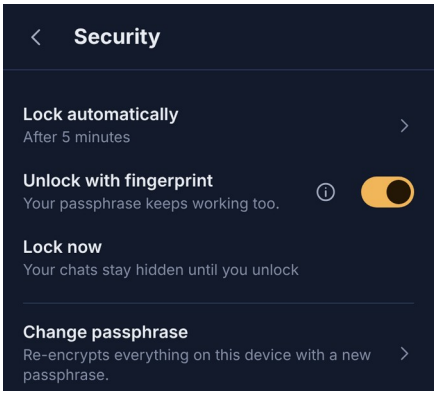

*Recluse is locked.*

## Fingerprint or Windows Hello (optional)

Instead of typing your passphrase every time, you can unlock with your fingerprint (Android) or with Windows Hello (Windows: your face, fingerprint or Windows PIN). Your passphrase keeps working too.

1. Open **Settings** (the gear icon at the top of the chat list), then **Security**.
2. Turn on **Unlock with fingerprint**. On Windows it is called **Unlock with Windows Hello**.
3. Enter your passphrase and tap **Turn on**.
4. Touch the sensor, or confirm with Windows Hello.

Next time, Recluse asks for your fingerprint by itself. Tap **Use passphrase** to type it instead.




*Settings, Security.*

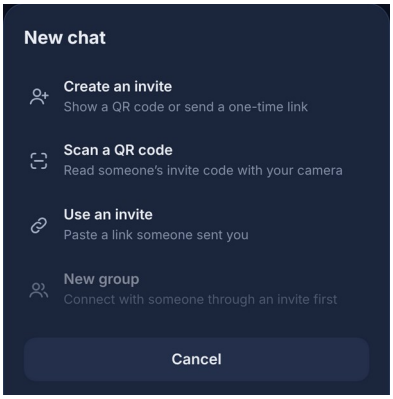
> **Good to know**
>
> - This option only appears if your phone or PC supports it.
> - If you add or remove a fingerprint on your phone, Recluse turns fingerprint unlock off for safety. Unlock with your passphrase, then turn it on again.
> - Someone could force your finger onto the sensor more easily than they could force a passphrase out of your head. Keep this in mind if that is a risk for you.

# 4. Add a contact

Recluse has no phone book. To talk to someone, one of you creates an **invite** and the other person uses it. An invite works once: the first person to open it becomes your contact. So give it only to the person you mean.

There are two ways to share an invite: show a **QR code** in person (the safest way), or send a **one-time link**. A QR code is the square black-and-white code that a camera can read.

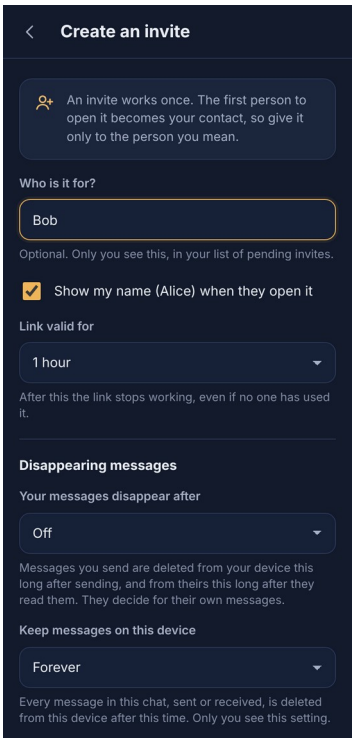
Everything starts with the **New chat** button at the bottom right of **Chats**. It shows four choices: **Create an invite**, **Scan a QR code**, **Use an invite** and **New group**.




*The New chat choices.*

## Create an invite

1. Tap **New chat**, then **Create an invite**.
2. **Who is it for?** Type a name, for example “Sara”. This is optional. Only you see it, in your list of pending invites.
3. Leave **Show my name … when they open it** ticked, so they know the invite is from you.
4. **Link valid for:** choose 10 minutes, 1 hour, 1 day or 1 week. After this time the link stops working, even if nobody used it. Choose the shortest time that works for you.
5. **Disappearing messages:** you can set timers for this chat now (chapter 7). If you are not sure, leave them as they are.
6. Tap **Create invite**.




*Create an invite.*

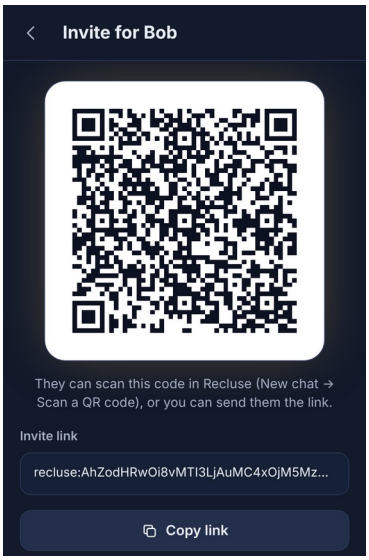
## Share the invite

Your invite now appears as a QR code and as a link.

- **In person:** the other person opens Recluse on their phone and scans your QR code (**New chat**, then **Scan a QR code**).
- **At a distance:** tap **Copy link** and send the link through a channel you trust (see the tip below).

Then tap **Done**. When the other person uses the invite, Recluse says **Your invite was answered** and opens your new chat.

Invites that are still waiting appear at the top of the chat list ("1 invite waiting for an answer"). Tap it to **Show** an invite again or to **Cancel** it. A cancelled link stops working right away.




*Your invite: QR code and link.*

> **Tip:** A "channel you trust" means a way where you are sure the link goes only to the right person: handing it over in person, or a chat where you know who is on the other side. You can send a link by SMS or WhatsApp, but anyone who sees it first could use it. That is why you compare safety numbers afterwards (see below).

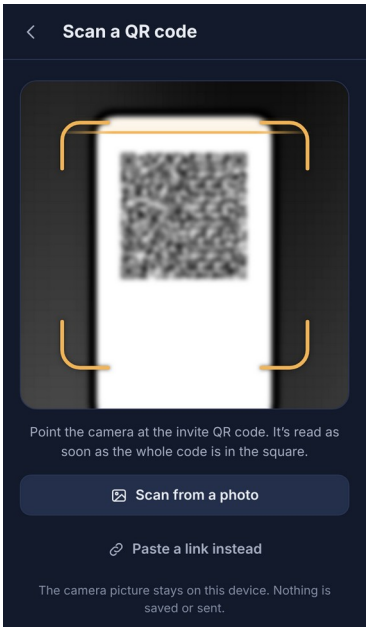
## Use an invite someone gave you

### Scan a QR code

1. Tap **New chat**, then **Scan a QR code**.
2. If your phone asks, allow Recluse to use the camera.
3. Point the camera at the invite QR code. It is read as soon as the whole code is inside the square.
4. You see **Invite from** and the person's name. Check that it is the right person. If you like, choose timers for disappearing messages.
5. Tap **Connect**.

**From a photo or screenshot:** on the scanner screen, tap **Scan from a photo** and choose the picture. This is useful on a PC without a camera, or when someone sent you a picture of their code.

The camera picture stays on your device. Nothing is saved or sent. Recluse only reads its own invite codes and never opens links from a QR code.



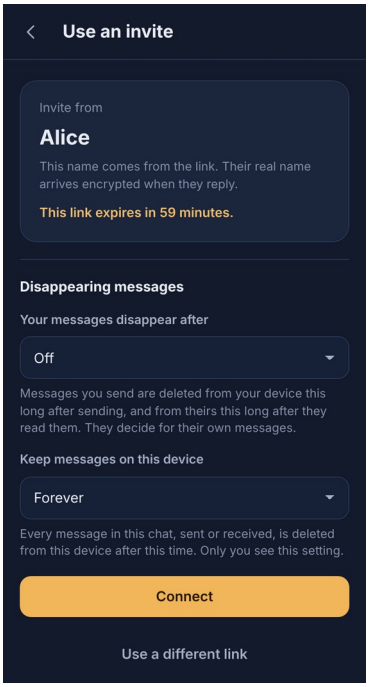

*Scan a QR code.*

### Paste a link

1. Copy the invite link. It starts with **recluse:**
2. In Recluse, tap **New chat**, then **Use an invite**.
3. Tap **Paste**, or paste the link into the box yourself. Tap **Continue**.
4. Check the name under **Invite from** and tap **Connect**.

The name you see comes from the link. Their real name arrives encrypted when they reply.

Right after connecting, the chat may say “Waiting for … to come online”. You can already write; your messages are delivered when they connect.



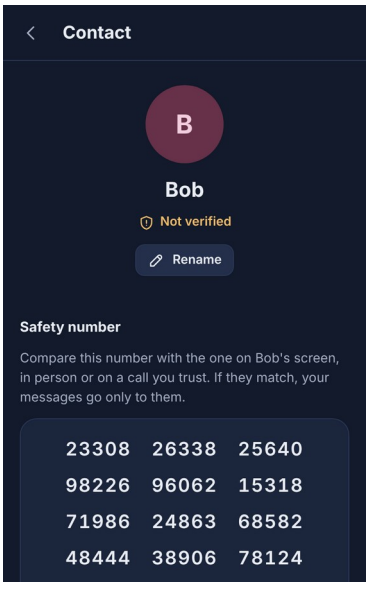

*Check who the invite is from, then Connect.*

> **Good to know:** If an invite doesn’t work, Recluse tells you why. For example:
>
> - “This invite link has expired. Ask for a new one.”
> - “You already used this invite.” (Recluse then opens that chat.)
> - “This is your own invite. Send it to the person you want to talk to.”
> - “This QR code isn’t a Recluse invite.”

## Safety numbers: make sure no one is in the middle

When an invite travels as a link, someone could copy it and secretly put themselves between you. Comparing **safety numbers** proves that you are really talking to each other. Until you do, the chat shows **Not verified** and a bar: “Compare safety numbers to be sure no one is in the middle.”

1. Open the chat and tap **Verify** in that bar, or tap the person’s name at the top of the chat.
2. Under **Safety number** you see 60 digits in 12 groups.
3. Compare them with the number on the other person’s screen. Both screens show the same number. Best: sit together. Or read the groups aloud to each other on a phone call where you recognise their voice.
4. If every group matches, turn on **Mark as verified**. The chat now shows **Verified** with a shield.




*The Contact screen with the safety number.*

> **Important:** If the numbers don’t match, don’t share anything private in that chat. Delete the chat, meet the person, and make a new invite face to face.
>
> If Recluse ever shows “This invite was answered twice”, someone else also used your link. It may have been copied. Compare safety numbers before you share anything sensitive.

# 5. Chatting

## Send a message

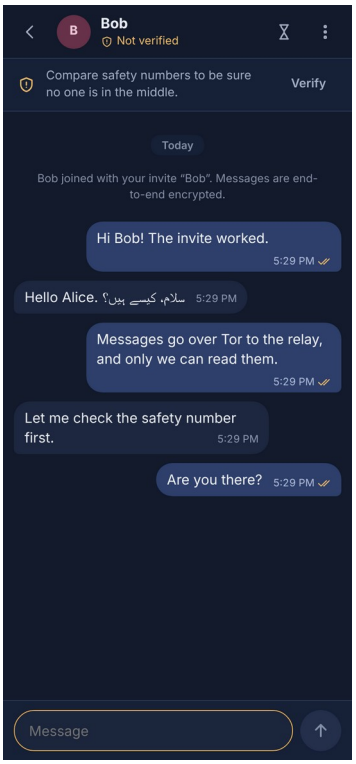
Type in the **Message** box at the bottom and tap the round arrow button. On a PC, press Enter to send; Shift and Enter together start a new line.

The small signs next to the time show what happened to your message:

- **Clock:** sending.
- **One tick:** sent. It has left your device.
- **Two ticks:** delivered to their device.
- **Two coloured ticks:** read. (Only if they have read receipts turned on.)
- **Red warning sign:** not sent. Tap the message and choose **Try again**.

If the other person is offline, your message waits for them on the **relay** (the mailbox server, see the glossary), locked so that nobody else can read it. It waits up to 14 days.

A small **hourglass** next to a message means it will disappear after a while (chapter 7).

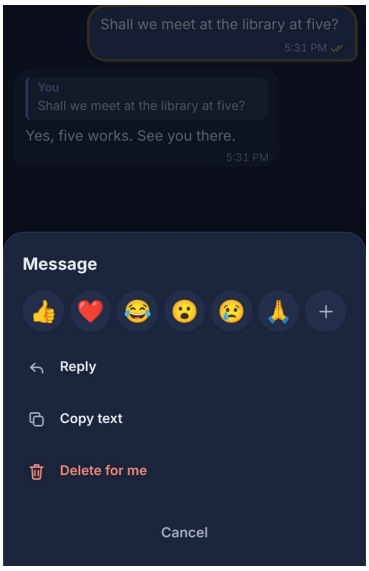



*A chat. The bar at the top suggests comparing safety numbers.*

## Reply, react, copy and delete

Tap a message to open its menu. On a PC, click it or right-click it.

- **React:** the row at the top has six quick reactions: thumbs up, heart, laughing, surprised, sad and thank you. The **+** button shows more. Each person can give one reaction per message. Tap your reaction again to take it back. Tap a reaction under a message to see who reacted.
- **Reply:** a “Replying to …” bar appears above the message box. On a phone you can also swipe a message to the right. Tap the **X** to cancel.
- **Copy text:** copies the message.
- **Delete for me:** removes the message from your device only.
- **Delete for everyone:** only for your own messages. It is removed here and from the other person’s device when it next connects.




*The message menu.*

## Read receipts and typing indicators

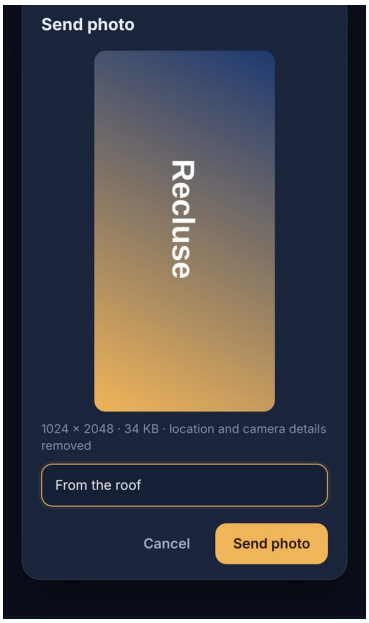
- **Read receipts** are on at first. They let your contacts see when you have read their messages. Turn them off in **Settings**, **Privacy**. When they are off, you don’t send them.
- **Typing indicators** (“… is typing”) are off at first. If you turn on **Send typing indicators**, the people you chat with see when you are typing. Your app then sends small encrypted messages while you type, so the relay can tell when you are active. They are never sent in groups of more than 10 members. The switch only controls what you send.
- Groups have no read receipts. Tap your own message in a group to see who it was sent to.

## Photos, voice notes and files

### Send a photo

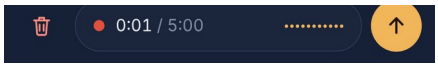
1. Tap the **paperclip** next to the message box, then **Photo**.
2. Choose a photo. You see a preview. Recluse removes the location and camera details hidden inside the photo.
3. Add a caption if you like, and tap **Send photo**.

Tap a photo in the chat to see it full screen. The arrow at the top saves it to your device.




*Sending a photo with a caption.*

### Send a voice note




*Recording a voice note.*

1. Leave the message box empty and tap the **microphone**. Allow the microphone if asked.
2. Speak. The clock shows how long you have recorded, up to 5 minutes.
3. Tap the **arrow** to send, or the **bin** to delete the recording.

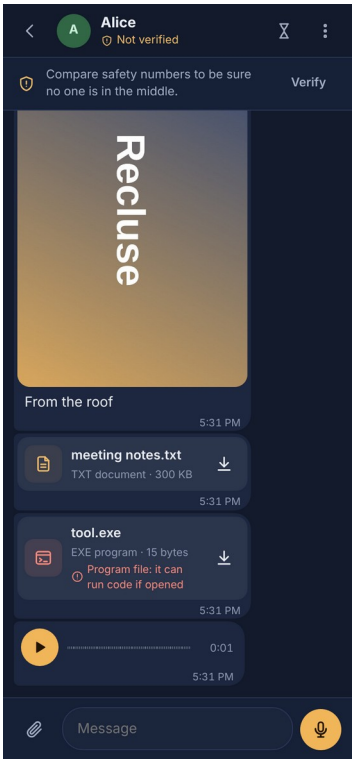
### Send a file

1. Tap the **paperclip**, then **File**.
2. Choose the file. Files are sent unchanged, up to 25 MB (5 MB in groups).
3. Add a caption if you like, and tap **Send file**.

### Save a file you received

Tap the download arrow on the file, or tap the message and choose **Save to device**. Recluse never opens files itself; it only saves them where you choose.

A program file (for example one ending in .exe) shows a red warning: “Program file: it can run code if opened.” Only open it if you trust the sender and expected it.




*A photo, two files and a voice note.*

> **Important:** A photo sent with **File** instead of **Photo** keeps its hidden details, such as where it was taken. To share a photo, use **Photo**.

## Limits

| What | Limit |
|---|---|
| **One message** | Up to 16,000 characters |
| **A file or photo in a chat** | Up to 25 MB |
| **A file or photo in a group** | Up to 5 MB |
| **A voice note** | Up to 5 minutes |
| **A group** | Up to 32 people, including you |
| **An invite link** | Valid for 10 minutes, 1 hour, 1 day or 1 week |
| **Messages waiting on the relay** | Kept for up to 14 days, then deleted |

### The Contact screen

Tap the person's name at the top of a chat to open **Contact**. Here you can **Rename** the contact (only you see this name), compare the **safety number**, and set **Disappearing messages** for this chat. **Delete chat** removes all messages and keys for this chat from your device; to talk again, you will need a new invite.

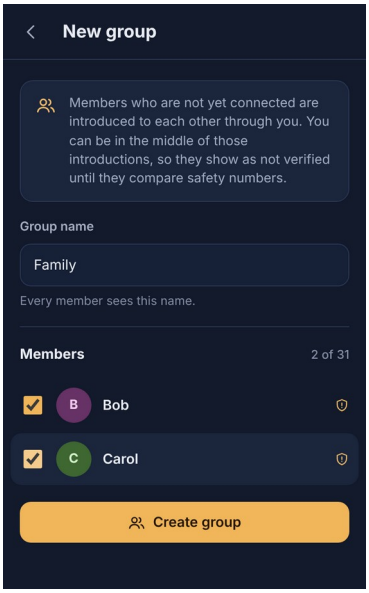
## 6. Groups

A group can have up to 32 people, including you. Messages are end-to-end encrypted between each pair of members. You can add people who are already your contacts.

### Create a group

1. Tap **New chat**, then **New group**. (You need at least one contact first.)
2. Type a **Group name**, for example "Family". Every member sees this name.
3. Tick the people you want to add. The counter shows how many you picked, for example "2 of 31".
4. Tap **Create group**.

You are now an **admin** of the group.




*New group.*

#### How members get to know each other

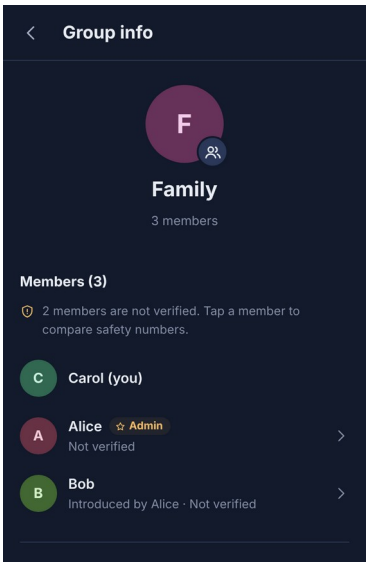
Members who are not yet connected are introduced to each other through you. Because you are in the middle of those introductions, they show as **Not verified** until they compare safety numbers. The group shows a bar: "Members you were introduced to aren't verified." Tap **Review**, tap a member, and choose **Safety number**.

### Group info

Tap the group name at the top of the group chat to open **Group info**.

- You see all **Members**. Admins have an **Admin** star.
- Tap a member for options: **Safety number**, **Message**, and for admins **Make admin** and **Remove from group**.
- Admins can also **Add members** and **Rename** the group.
- New members see messages sent from then on, not earlier ones.
- **Your disappearing timer** and **Keep messages on this device** work like in a normal chat (chapter 7). Each member sets their own timer.
- **Leave group:** you stop getting messages from the group. You can still read what is already there. Afterwards you can **Delete group** to remove it from your device.

Someone who is removed from a group keeps the messages they already have.




*Group info.*

## 7. Disappearing messages and privacy options

Every chat has two separate timers. You choose them when you create or use an invite, and you can change them at any time.

#### Your messages disappear after

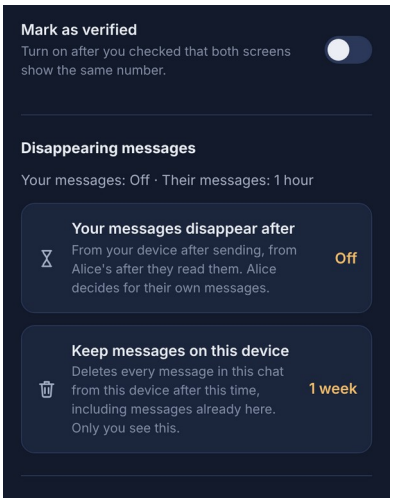
This is your timer for the messages **you send**. They are deleted from your device that long after sending, and from the other person's device that long after they read them. The other person decides for their own messages. Choices: Off, 5 minutes, 1 hour, 1 day, 1 week.

#### Keep messages on this device

This deletes **every** message in the chat, sent or received, from **your** device after the time you choose. It also applies to messages already in the chat. Only you see this setting. Choices: Forever, 5 minutes, 1 hour, 1 day, 1 week.

#### Where to change them

- **In a chat:** tap the **hourglass** at the top. Or tap the name and scroll to **Disappearing messages**.
- **In a group:** open **Group info** and use **Your disappearing timer**.
- **For all new chats: Settings**, **Disappearing messages**. These are preselected when you create or use an invite. Existing chats keep their settings.




*Both timers on the Contact screen.*

> **Important:** Disappearing messages can't stop the other person from photographing their screen with another phone before a message disappears.

## When the screen turns off

In **Settings**, **Privacy** you can tell Recluse to clean up whenever your phone screen turns off. On Windows this option is called **When the PC locks or sleeps**. The choices are:

| Choice | What happens |
|---|---|
| **Do nothing** | Messages stay until you delete them or a timer does. This is the normal setting. |
| **Clear read messages** | Deletes the chat history from this device, in every chat and group. Unread messages stay until you have seen them, and messages not sent yet stay until they are sent. Contacts and groups stay. |
| **Clear all messages** | Deletes every message in every chat and group, unread ones too. Contacts and groups stay. |
| **Wipe everything** | Deletes everything on this device, like **Delete everything** in Settings: your identity, contacts, groups, messages and keys. To turn it on you must type WIPE. |

If Recluse is locked at that moment, the messages are cleared the next time you unlock, before any chat is shown. It also happens after Recluse restarts.

> **Important:** **Wipe everything** really means everything, every time the screen turns off and every time Recluse restarts. Nothing can be recovered, and your contacts will need a new invite to reach you. Only choose it if you are in serious danger.

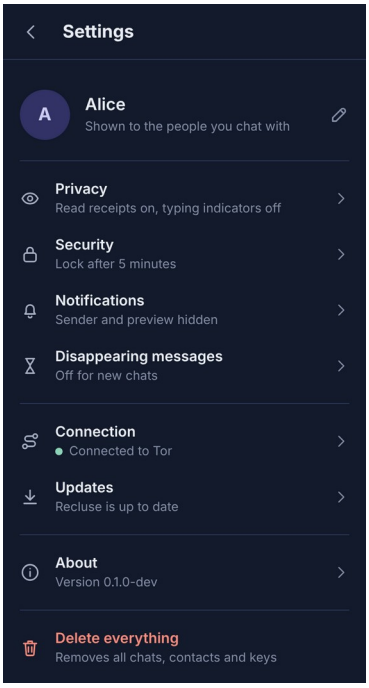
**Screenshots:** Recluse blocks screenshots of its own screen. On Android it also hides its content in the list of recent apps.

# 8. Settings, page by page

Tap the **gear** icon at the top of the chat list to open **Settings**. At the top is your **name**: tap it to change it. Below it is a short list of pages, and **Delete everything** in red at the end.

Under each item a short line shows how it is set, for example “Lock after 5 minutes”. Tap an item to open its page, and tap the back arrow to return.

Many settings have an **(i)** button. Tap it to read a fuller explanation, then tap **OK**.

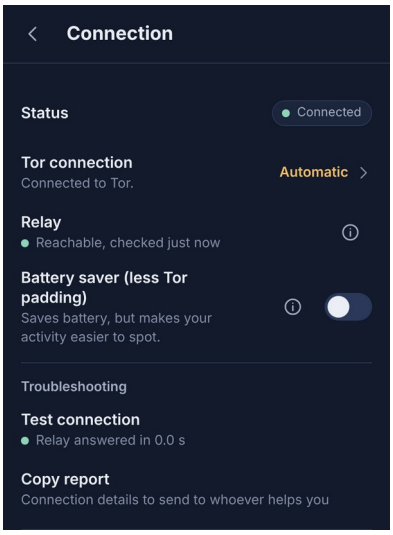



*The Settings list.*

| Page | What you find there |
|---|---|
| **Privacy** | **Read receipts** (on at first) and **Send typing indicators** (off at first): see chapter 5. **When the screen turns off** (on Windows: **When the PC locks or sleeps**): see chapter 7. |
| **Security** | **Lock automatically:** after 1, 5, 15 or 30 minutes, after 1 hour, or never (at first: after 5 minutes). **Unlock with fingerprint** or **Unlock with Windows Hello** (chapter 3). **Lock now**. **Change passphrase:** type your current passphrase, then the new one twice, and tap **Change passphrase**. |
| **Notifications** | At first a notification only says “New message”. **Show who it’s from** adds the sender’s name; **Show a preview** then adds the start of the message. Anyone who can see your screen can read a preview. On Android this page also has the **Delivery** settings (chapter 10). |
| **Disappearing messages** | The timers preselected for **new** chats (chapter 7). Existing chats keep their settings. |
| **Connection** | **Status**, **Tor connection** (the bridges, chapter 9), **Relay** (whether Recluse can reach its server), **Battery saver** (below), **Test connection** and **Copy report** (chapter 9), and under **Advanced** the **Relay address**. Recluse fills in the relay address for you; you don’t need to change it. |
| **Updates** | Your version, **Check now**, and **Check for updates automatically** (chapter 11). |
| **About** | Your version, and the links **Download site** and **Verify a download**. They open in your web browser, which does not use Tor. |

### Battery saver (less Tor padding)

Off at first. Tor normally sends a little filler traffic every few seconds. This makes it harder for someone watching your connection, such as your mobile operator, to tell when you are messaging, but it keeps the phone's radio awake. Battery saver sends much less filler, so the battery lasts longer, but that protection gets weaker. Messages stay end-to-end encrypted either way.




*Settings, Connection.*

### Delete everything

1. Tap **Delete everything**.
2. Read the warning and tap **Continue**.
3. Type **DELETE** and tap **Delete everything**.

> **Important:** All chats, contacts, invites and keys on this device are deleted, and Recluse closes. This cannot be undone. Your contacts will need a new invite to reach you. (Uninstalling Recluse on Windows does not delete your data. Use Delete everything if you want it gone.)

# 9. Connection and bridges

In some places, internet companies block Tor. A **bridge** is a hidden entrance to Tor that is harder to block. Bridges disguise Tor traffic so it looks like something else.

## Do I need to do anything?

Usually not. In **Automatic** mode (the recommended setting), Recluse tries a direct connection first, then each type of bridge, until one works. It starts with the way that worked last time on your device. A way only counts as working once Recluse's server has actually answered through it.

Some networks, often university, school or office Wi-Fi, block Tor's public bridges in a sneaky way: Tor seems to connect, but nothing gets through. Recluse notices that its server never answers and moves on to the next kind of connection by itself, within about two minutes, starting with its own **WebTunnel** bridge. When you switch between Wi-Fi and mobile data, Recluse reconnects Tor by itself too.

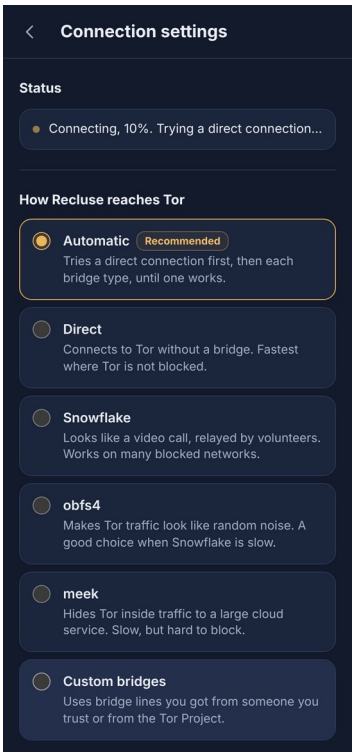
> **Tip:** On university or office Wi-Fi you can save those two minutes: open **Settings**, **Connection**, **Tor connection**, choose **WebTunnel** and tap **Save and reconnect**. Switch back to **Automatic** at home.

## Choose a bridge yourself

1. Open **Settings**, **Connection**, **Tor connection**. Or tap **Connection settings** on the “Connecting to Tor” box or on the lock screen.
2. Under **How Recluse reaches Tor**, choose one of the options below.
3. Tap **Save and reconnect**.

**Status** at the top shows what is happening, for example “Connected through a Snowflake bridge.”

If you are stuck, a good order to try is: **Automatic**, then **WebTunnel**, then **Snowflake**, then **obfs4**, then **meek**. Give each one a few minutes.




*Connection settings. Your list also includes WebTunnel.*

| Option | What it does |
|---|---|
| **Automatic (Recommended)** | Tries a direct connection first, then each bridge type, until one works. |
| **Direct** | Connects to Tor without a bridge. Fastest where Tor is not blocked. |
| **WebTunnel** | Looks like visiting an ordinary website. Recluse’s own bridge. |
| **Snowflake** | Looks like a video call, relayed by volunteers. Works on many blocked networks. |
| **obfs4** | Makes Tor traffic look like random noise. A good choice when Snowflake is slow. |
| **meek** | Hides Tor inside traffic to a large cloud service. Slow, but hard to block. |
| **Custom bridges** | Uses bridge lines you got from someone you trust or from the Tor Project. Paste one bridge per line, starting with obfs4, webtunnel, snowflake or meek_lite. Up to 20 lines. |

These settings are kept on your device outside the locked vault, because Tor has to start before you unlock. **Delete everything** removes them too.

## What the connection status means

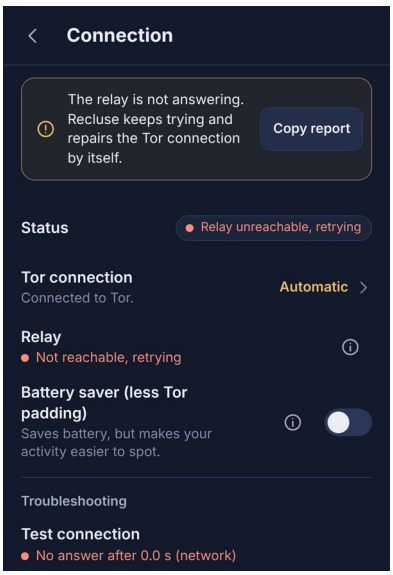
| You see | It means |
|---|---|
| **Connected** | Everything works. (“Sending” while messages are going out.) |
| **Connecting to Tor 40%** | Tor is still starting. |

| You see | It means |
|---|---|
| **Reaching relay…** | Tor is ready and Recluse is checking that its server (the relay) answers. |
| **Relay unreachable, retrying** | Tor works, but the relay doesn’t answer. Recluse keeps trying and repairs the connection by itself: new paths through Tor after 45 seconds, then a fresh Tor connection, in Automatic mode through the next kind of connection. |
| **No internet connection** | Your device is offline. Recluse connects again as soon as it is back online. |
| **Tor is not running** | Tor stopped. See chapter 12. |

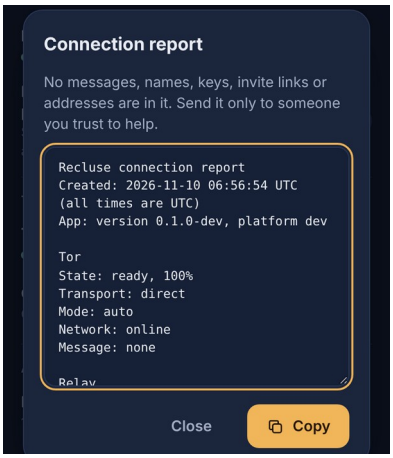
## Check the connection and send a report

1. Open **Settings**, **Connection**. The **Relay** line shows whether Recluse can reach its server, for example “Reachable, checked 2 min ago” or “Not reachable, retrying”.
2. Tap **Test connection**. Recluse asks the relay to answer right now and shows how long it took, for example “Relay answered in 4.2 s”.
3. If something keeps going wrong, tap **Copy report**, then **Copy**. Paste it into the feedback form on the website (chapter 13), or send it to the person who helps you.

The report lists only connection details: the state of Tor, which kinds of connection were tried, errors and times. It never contains messages, names, keys, invite links or addresses.




*When the relay doesn’t answer.*




*The connection report (example from a test copy).*

# 10. Notifications on Android

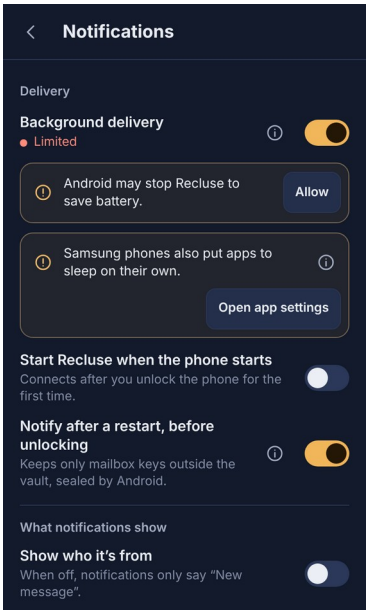
Most apps get their notifications through Google. Recluse doesn't, because that would tell Google when someone writes to you. Instead, Recluse keeps its own connection open in the background. Android sometimes stops such apps to save battery, so a few settings help your messages arrive on time.

While Recluse runs, you see a quiet notification: **Recluse – Connected through Tor**. This is normal. It keeps Recluse running so messages can arrive. Its **Quit** button stops Recluse completely; then no messages arrive until you open Recluse again.

## Make sure messages arrive

1. Open **Settings**, **Notifications**.
2. Make sure **Background delivery** is on. The line under it says **Fully allowed** or **Limited**.
3. If you see "Android may stop Recluse to save battery", tap **Allow** and confirm. Android then stops putting Recluse to sleep (this is called a battery exemption).
4. If you see "Android does not let Recluse show notifications", tap **Allow**.
5. On a **Samsung** phone you also see "Samsung phones also put apps to sleep on their own." Tap **Open app settings**, then: **Battery**, choose **Unrestricted**. Also make sure Recluse is not in **Sleeping apps** or **Deep sleeping apps** (Samsung **Settings**, **Battery**, **Background usage limits**).

When nothing is limited any more, it says **Fully allowed**.




*Settings, Notifications on Android.*

> **Tip:** Other phone brands also have their own battery savers, with different names. If messages arrive late, look in your phone's **Settings**, **Apps**, **Recluse**, **Battery** for an option such as "Unrestricted" or "Allow background activity".

## Two more options

- **Start Recluse when the phone starts** (off at first): Recluse connects after you unlock the phone for the first time.
- **Notify after a restart, before unlocking** (on at first): after the phone restarts, you get "New message" alerts even before you unlock Recluse. For this, Recluse keeps only its mailbox keys (never messages or contacts) outside the vault, sealed by Android. Turn it off for the strictest privacy.

If you ever see the notification "Recluse was stopped. New messages can't arrive. Tap to reconnect.", tap it, then check steps 3 to 5 above.

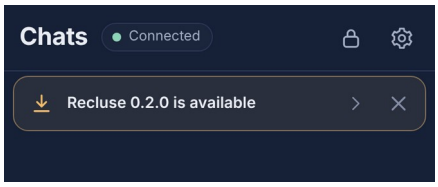
**On Windows**, Recluse shows notifications while it runs, also when its window is closed and it sits in the tray. The **What notifications show** settings work the same way there.

# 11. Updates

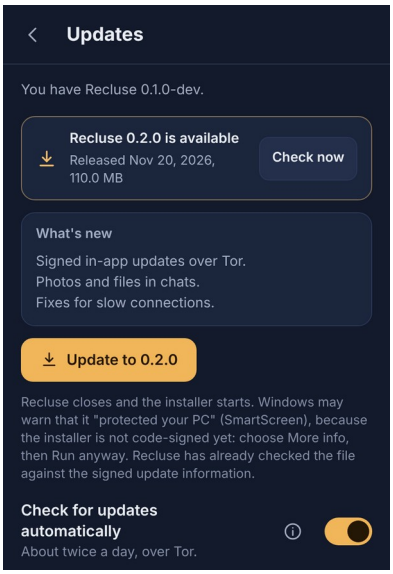
Recluse checks for new versions by itself, about twice a day, over Tor. Updates are **signed**: Recluse checks the digital signature and the downloaded file before it installs anything, so a fake update is refused.

1. When an update is ready, a bar appears above your chats: “Recluse … is available”. Tap it. (Or open **Settings**, **Updates**.)
2. Read **What’s new**.
3. Tap the **Update to …** button. Recluse downloads the update over Tor and checks it.
4. Then it depends on your device:
   - **Android:** Android asks you to confirm. The first time, Recluse may say **Allow Recluse to install updates**. Tap **Open settings**, turn on **Allow from this source** for Recluse, come back and tap **Install now**.
   - **Windows installer:** tap **Install and close**. Recluse closes and the installer starts. If SmartScreen warns, click **More info**, then **Run anyway**.
   - **Windows portable:** tap **Save and close**. The new version is saved next to the old file and Recluse closes. Start the new file. Your chats stay in the Recluse Data folder.

To check yourself, open **Settings**, **Updates** and tap **Check now**. The switch **Check for updates automatically** is on at first. The check goes over Tor, so it never reveals your IP address.




*The update bar in the chat list.*




*Settings, Updates (example from a test copy).*

> **Important:** On Android, if an update ever fails with “App not installed”, don’t uninstall Recluse to get around it. Uninstalling deletes your messages, and the update may not be genuine. Download it again from get.freedomwithrahi.trade and check it.

## What’s new in version 0.2.3

- Fixed: after Tor reconnected or you changed the connection, “Could not reach the relay” could stay until Recluse was restarted.
- On networks that block Tor’s public bridges (often university or office Wi-Fi), Recluse moves on to the next kind of connection by itself, starting with its own WebTunnel bridge.
- Moving between Wi-Fi and mobile data reconnects Tor straight away.
- Chats open at your latest message.
- A photo deleted for everyone while it was still on its way no longer flashes up on the other phone.
- Fixed: the first screens could slide sideways on many phones, and some phones (for example Xiaomi Redmi) recoloured Recluse with their own dark mode.
- Fixed: **Quit** in the notification could crash the app.

### And in version 0.2.2

- Recluse checks that its server really answers, and the status says **Reaching relay…** or **Relay unreachable, retrying** instead of a misleading “Connected”.
- It repairs the Tor connection by itself, and creating or accepting an invite keeps trying for up to two minutes.
- **Settings**, **Connection** shows the relay’s state, with **Test connection** and **Copy report**.
- Recluse locks when you close it (chapter 3).

# 12. Problems and how to fix them

### “Connecting to Tor” takes a long time

- Wait a few minutes. On slow or restricted networks this is normal.
- Check that your internet works, for example by opening a website in your browser. If you can, try switching between mobile data and Wi-Fi.
- If the box says “Your network may be blocking Tor”, Recluse is already trying bridges in Automatic mode. Give it a few more minutes.
- Still stuck? Tap **Connection settings** and choose a bridge yourself: try **WebTunnel**, then **Snowflake**, then **obfs4**, then **meek**. Tap **Save and reconnect** (chapter 9).

### It says “Could not reach the relay” or “Relay unreachable, retrying”

The relay is the mailbox server where messages wait. Tor can be connected while the relay still doesn’t answer.

- Make sure you have **version 0.2.3** or newer (**Settings**, **About**). It fixed the most common cause.
- Wait about two minutes. Recluse retries by itself, repairs the Tor connection, and in Automatic mode tries the next kind of connection. Creating an invite keeps trying for up to two minutes as well.
- On university, school or office Wi-Fi: choose **WebTunnel** in **Settings**, **Connection**, **Tor connection**, or switch to mobile data.
- Still failing? Open **Settings**, **Connection**, tap **Test connection**, then **Copy report**, and send the report with the feedback form (chapter 13).

### It says “Tor could not start”

- **Android:** tap **Restart Recluse**. Your chats stay; you unlock again after the restart.
- **Windows:** right-click the Recluse icon in the tray, choose **Quit Recluse**, and open Recluse again.

### Messages or notifications arrive late (Android)

- Open **Settings**, **Notifications**. **Background delivery** should be on and say **Fully allowed**. Tap **Allow** on any warning there (chapter 10 has the extra steps for Samsung).
- Don’t tap **Quit** on the Recluse notification, and don’t use **Force stop** in Android’s app settings. Both stop Recluse until you open it again.

### I forgot my passphrase

We are sorry: there is no way to get it back. This is also what keeps your chats safe, because nobody else can get in either.

- First, try calmly a few more times. Check that Caps Lock is off and that your keyboard is set to the right language (for example English, not Urdu).

- If you really can't remember it: on the lock screen, tap **Forgot your passphrase?** and then **Delete everything...** Then type **DELETE** and tap **Delete everything**.
- Set up Recluse again with a new passphrase, and send new invites to your contacts. Your old messages are gone.

### I have a new phone, or I want to use Recluse on another device

Each device is a separate identity in Recluse. There is no syncing and no backup, so chats can't be moved to another device. Your phone and your PC can both run Recluse, but they are two separate "you"s: your contacts add each one separately.

To move to a new phone:

1. Install Recluse on the new phone and set it up as new.
2. While you still have the old phone: on the new phone, create one invite for each contact. Send each link to that person through your **old** Recluse chat with them. That chat is a channel you trust.
3. Each contact uses the invite. Compare safety numbers again.
4. When everyone is connected to your new phone, open **Settings** on the old phone and tap **Delete everything**. Your contacts can delete their old chat with you.

### My invite expired or didn't work

Create a new invite and share it again. If the other person sees "The invite expired before your answer was delivered", they should ask you for a new invite and delete the chat that couldn't connect.

### The camera doesn't work when I scan a code

- If Recluse says it isn't allowed to use the camera: on **Android**, open your phone's **Settings**, **Apps**, **Recluse**, **Permissions**, **Camera** and choose **Allow**. On **Windows**, open **Settings**, **Privacy & security**, **Camera** (on Windows 10: **Privacy**, **Camera**) and turn on camera access and **Let desktop apps access your camera**.
- Or use **Scan from a photo**, or ask for the link and paste it.

### Recluse looks wrong, slides sideways or has odd colours

Version 0.2.3 fixed screens that could be dragged sideways on many phones, and phones (such as Xiaomi Redmi) that recoloured Recluse with their own dark mode. Update first. If it still looks wrong, take a photo of the screen with another phone and send it with the feedback form (chapter 13), together with the phone's model.

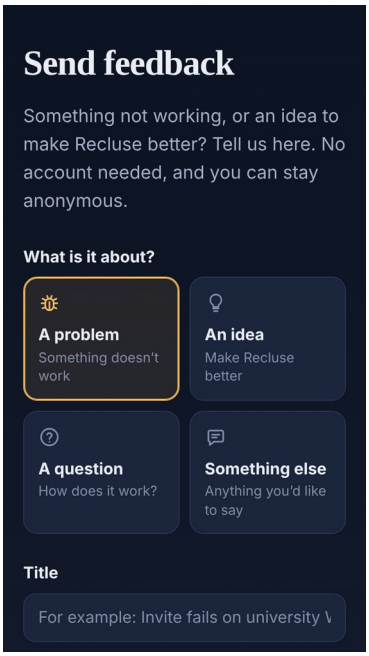
### Windows says "Windows protected your PC", or a message says "Not sent"

**Windows protected your PC:** click **More info**, then **Run anyway** (see chapter 2). **Not sent:** check your connection, tap the message and choose **Try again**.

## 13. Feedback and help

Found a problem, or have an idea to make Recluse better? Tell us on the website. You don't need an account, and you can stay anonymous.

1. In your browser, open **get.freedomwithrahi.trade/feedback** (or tap **Feedback** at the top of the website).
2. Choose what it is about: **A problem**, **An idea**, **A question** or **Something else**.
3. Give it a short **title**, then describe it. For a problem, say what you did, what happened and what you expected. You can also list the steps that make it happen.
4. If you like, add your device: Android or Windows, the app version (**Settings**, **About**), your phone or PC model, and which internet you were on.
5. For connection problems, open **Add a connection report** and paste the report from Recluse (chapter 9).
6. Add up to **4 photos** if they help. Recluse blocks screenshots, so take a photo of the screen with another phone.
7. If you want an answer, write an email address or another way to reach you. Leave it empty to stay anonymous.
8. Tap **Send feedback**. You get a **reference** such as RCL-7K3F9QPM. Keep it if you want to ask about it later.




*The feedback form on the website.*

> **Important:** Never write your passphrase, invite links or private messages in the form. The form doesn't store your IP address, the website sets no cookies, and location and camera details are removed from photos before they are sent.

## 14. Staying safe

Recluse protects your messages on the way and on your device. But no app can protect against everything. Here is what Recluse **can't** protect against, in plain words:

| Risk | What it means for you |
|---|---|
| **Spyware on your phone or PC** | If your device has a hidden spying app, it can read your messages on the screen after Recluse unlocks them. Keep your device updated and only install apps you trust. |
| **Someone with your unlocked phone** | Anyone holding your phone or PC while Recluse is unlocked can read your chats. Lock Recluse when you put it down, and use a strong passphrase. |
| **The person you are talking to** | Recluse blocks screenshots, but a contact can still photograph their screen with another phone, or tell others what you wrote. Encryption can't make someone trustworthy. |
| **Mistakes not found yet** | Recluse uses well-known, tested encryption, but Recluse itself hasn't had an independent security audit yet. Treat it as new software. |
| **Someone watching most of the internet** | A very powerful observer who can watch large parts of the Tor network at once may be able to match up the timing of traffic. Tor can't fully prevent that. |

### Ten good habits

1. Download Recluse only from **get.freedomwithrahi.trade**.
2. Compare **safety numbers** with the people who matter most, in person if you can.
3. Send invite links only through channels you trust, with a short **Link valid for** time.
4. Choose a strong **passphrase**, keep it secret, and keep **Lock automatically** short.
5. Lock Recluse with the **padlock** when you put your device down, and lock your phone with a PIN.
6. Use **disappearing messages** for sensitive chats.
7. Keep notifications private: leave **Show who it's from** and **Show a preview** off.
8. Send photos with **Photo**, not **File**, so their hidden location details are removed.
9. Don't open program files unless you trust the sender and expected the file.
10. Keep Recluse up to date. Install updates when Recluse offers them.

## 15. Glossary

| Word | What it means |
|---|---|
| **Tor** | A free network run by volunteers. It sends your traffic through several computers around the world, so nobody can easily see where it comes from or where it goes. Recluse only talks through Tor. |
| **Bridge** | A hidden entrance to Tor. Bridges help where Tor is blocked, because they make Tor traffic look like something else. Recluse can choose one for you. |
| **Relay** | The mailbox server where your messages wait until the other person's device collects them. It only holds locked messages. It can't read them, and it never learns your IP address, your name or who your contacts are. Messages that nobody collects are deleted after 14 days. |
| **Invite** | A one-time QR code or link that connects you with one person. The first person to use it becomes your contact. It stops working after the time you chose. |
| **Safety number** | A 60-digit number that both of you see in your chat. If the numbers on both screens match, nobody is secretly in the middle. |
| **Passphrase** | A long password made of several words. It locks everything Recluse keeps on your device. Nobody can recover it if you forget it. |
| **Vault** | The locked storage on your device where Recluse keeps your chats, contacts and keys. Only your passphrase (or your fingerprint or Windows Hello, if you turned that on) opens it. |
| **End-to-end encryption** | Your message is locked on your device and only unlocked on the other person's device. Nobody in between can read it. |
| **Checksum** | A fingerprint of a file. If it matches the one on the website, the file is genuine. |
| **Connection report** | A short list of connection details (**Settings**, **Connection**, **Copy report**) that helps find connection problems. It contains no messages, names, keys, invite links or addresses. |