Afghan Witness

DIGITAL SAFETY FOR WOMEN & GIRLS

This guide has been created to empower you with the knowledge and tools needed to protect your digital presence. While it is primarily aimed at Afghanistan's women and girls, the advice is applicable to anyone.

In an environment where freedom is restricted, social media and other digital forms of communication become crucial methods of participation. Digital security and privacy are often at risk, however, and individuals can be identified based on their online activities, communications, or other digital data.

Whether you are seeking education, connecting with others, or simply navigating the internet, understanding how to secure your online activities is extremely important. By following the practices outlined here, you can enhance your privacy, safeguard your personal information, and confidently engage in the digital world, despite the challenging circumstances you face.

YOU'RE ONLY AS STRONG AS YOUR WEAKEST LINK.

TABLE OF CONTENTS

01. IDENTIFYING YOUR SECURITY RISKS

THREAT ORIGIN

To protect yourself, you need to understand the risks you face.

Think of where a threat might come from:

- A family member stalking your social media profiles.
- An unwanted suitor pursuing you romantically.
- Authorities stopping you and checking your phone.
- An influential person interested in you.
- Unknown people targeting you because of your online posts.

Each of these situations presents **different security risks.** The measures to protect yourself from a random phone check are different from those needed to hide from angry internet users or powerful authorities trying to identify you.

The risk depends on how much the 'threat actor' (the person threatening you) knows about you, how strong their resources, influence, and tech skills are. Regardless of where the threat comes from, **it's always best to take maximum precautions.**

ENVIRONMENT

The security risks you face depend on **where you live**.

In the USA or Europe, laws protect your personal data. Generally, the content of your devices or your online activity history is not easily accessible unless you are considered a serious criminal or security threat by the courts.

In these locations, your main risks involve: the information you share on online platforms, your devices being hacked remotely, or someone in your immediate environment accessing your device.

In a context such as **Afghanistan**, the situation is different.

Without legal protections, not only your social media posts but also your internet traffic and **any information** on your devices can be security risks.

Afghan authorities have a large amount of biometric data on people involved with the former government and the U.S. government, as well as a lot more data on the population at large, which they use to identify local activists, journalists, and others.

Here, threats may come from a jealous individual with limited tech skills or from a security agency with extensive information and expertise. **Do not underestimate the technological capabilities of someone looking to harm or track you online.**

DIFFERENT STRATEGIES

Different threat scenarios may require different strategies and levels of protection.

Here are two examples to illustrate this:

HIGH SKILLS - NO PHYSICAL ACCESS

If your 'threat actor' has high technological skills but no direct physical access to your device, it is crucial to:

- Use **privacy-focused apps** for communication
- Employ tools like a VPN or the Tor browser to **hide your internet traffic**
- **Protect** your devices against **hacking**
- **Maximise** your privacy settings on **social media**

LOW SKILLS - PHYSICAL ACCESS

If your threat actor has low technological skills but might have direct physical access to your device, you need to hide sensitive information in ways that are not easily detectable. This can include:

- Using unusual apps, **coded language**, or **flooding your device with harmless data** like multiple chat groups or pictures about kittens.
- You can also **hide sensitive data on an external drive** or cloud service to make it harder for them to find anything they could use to harm you.

Maximising your privacy and security is crucial, especially if you are unsure where the threat may come from.

However, it is also important to **avoid triggering suspicion** by having **too many** privacy-focused apps, or a **completely clean device** without any data, if someone gains access to your device.

Personal judgement on what the **right balance** looks like in your context is important here.

SOCIAL ENGINEERING

WHAT IS SOCIAL ENGINEERING?

Social engineering is a tactic used by attackers to trick you into giving away your personal information. These attackers might pretend to be someone you trust, such as a friend, family member, or even a company you know.

COMMON SOCIAL ENGINEERING TACTICS

Impersonation: Someone might pretend to be a friend or a relative in need of help. They could ask you to send money or share personal details. Be wary if someone you know does not communicate with you as they normally would.

Urgency: Attackers might create a sense of urgency, claiming that something bad will happen if you don't act quickly. For example, they might say *"Your account will be locked unless you provide your password immediately!"*

WHAT IS PHISHING?

Phishing is a type of social engineering where attackers send fake messages to trick you into revealing sensitive information.

These messages can come through email, text, social media, or calls.

COMMON SIGNS OF PHISHING

Suspicious Links: Be cautious of links in messages that ask you to log in or provide personal information. These links might lead to fake websites that look real but are designed to steal your information.

Unusual Requests: Be wary of messages that ask for personal details, passwords, or financial information. Legitimate companies and organisations typically do not ask for sensitive information this way.

Poor Language: Many phishing messages contain spelling and grammar mistakes or use language that seems odd.

HOW TO PROTECT YOURSELF

Verify the Source: If you receive a suspicious message, contact the person or organisation directly using a known, trusted method (like a phone number, email address or direct contact you already have).

Don't Click on Suspicious Links: Hover your mouse over links to see where they lead before clicking. If the link looks strange or doesn't match the sender's usual website, don't click it.

Use Security Software: Install and update security software on your devices. This can help detect and block malicious messages and websites.

WHAT TO DO IF YOU SUSPECT A PHISHING ATTEMPT

Do Not Respond: If you receive a suspicious message, do not reply or click on any links.

Report It: Report the message to the platform where you received it. For example, if it came through email, you can mark it as 'spam' or 'phishing'.

Change Your Passwords: If you think you might have fallen for a phishing attempt, change your passwords immediately to prevent further access to your accounts.

02. SECURING APPS AND DEVICES

YOUR DEVICES CAN BE UNSAFE

Your devices, such as your phone or laptop, **track** your location, your data and your behaviour by default. This can be accessed by someone who has **hacked** your device, or by **authorities** if they possess the necessary expertise. If someone accesses your device, they can **easily search through all your information** and communications through apps such as WhatsApp.

MOBILE DEVICE ENCRYPTION

Making sure that your phone is **encrypted** is crucial to protect your data if your device is lost or stolen. Encryption converts your data into a format that can only be read with the correct 'decryption key', which is typically tied to your phone's **password or PIN**. **Ensure you have a strong passcode** to maximise security.

iPhones are **encrypted by default** when you set a passcode. On **Android models 10** and higher, the device is also **encrypted by default**. On older models, encryption must be enabled manually.

On older Android models, you can check whether your phone is encrypted by navigating to **Settings > Security > Encryption.**

If your device is not encrypted, you can enable encryption from the same tab (Settings > Security > Encryption.),

However, note that the process takes 1-2 hours and requires a full charge – if your device accidentally shuts down before the process is complete, your phone will no longer work: you will have to reset the device and you risk losing your data.

USE SECURE MESSAGING APPS

Calling over the **normal phone network** or **sending SMS** is very **unsafe** because the contents of your communications can be **easily intercepted.** It is safer to use secure messaging platforms like **WhatsApp** or **Signal**.

Signal is one of the most secure messaging apps. It offers end-to-end encryption, meaning only you and the person you're communicating with can read the messages. Signal is also open-source, meaning that its code is publicly available for experts to inspect how it functions, ensuring transparency and trust.

WhatsApp also offers end-to-end encryption for messages, calls, photos, and videos. It's user-friendly and widely used, making it a convenient choice for secure communication.

To enhance security, enable additional features like **two-step verification**, **disappearing messages**, and **app locks**, as you will be shown in the next pages. Be cautious about sharing your number publicly and **regularly review your privacy settings** to control who can see your information.

SECURING YOUR PC

Securing your computer is crucial for protecting your personal data and maintaining privacy, especially in sensitive situations. Install **reputable antivirus** software and **enable your firewall** to guard against malware and unauthorised access. **Regularly update** your operating system and applications **to fix security vulnerabilities.**

PROTECT AGAINST MALWARE

Antivirus

For most purposes, if you are using a Windows computer, the built-in Windows Defender software is secure enough – as long as you keep it up to date and activated. If you want some additional features, a good option is Bitdefender, which has both free and paid options.

For Mac, the default antivirus is also generally secure enough. But if you seek additional security, Malwarebytes offers a free virus scanner and antivirus.

Do not use more than one antivirus - they may block each other from working properly.

Firewall

Firewalls are an essential component of your computer's security, acting as a **barrier** between your device and potential threats from the internet. A firewall **monitors and controls** incoming and outgoing network traffic based on predetermined security rules. It acts as a filter, allowing safe traffic through while **blocking harmful or suspicious traffic.**

Windows and Mac both have a **built-in firewall,** which provides a basic level of protection by monitoring and filtering traffic. It's easy to configure and manage through the **Windows Security settings**, or in the **Security & Privacy settings** for Mac.

On Windows 10 or 11, click the Start button, go to **Settings > Update & Security > Windows Security > 'Firewall & network protection'**. Here, you'll find the status of your Windows Firewall. **Ensure it's set to 'On'.**

If you are trying to find more security and control beyond the built-in firewall, you can choose Tinywall for Windows (free) and Little Snitch for Mac (paid).

Updates

Keeping your software updated is one of the most **crucial steps** in maintaining digital security. Regular updates help protect your devices from the latest threats and ensure that your systems run smoothly.

New vulnerabilities are constantly discovered in software, and hackers are quick to develop ways of exploiting them. Software updates often include fixes for these newly discovered vulnerabilities. **By regularly updating your software, you close the security gaps that a hacker might exploit.**

GENERAL TIPS

- Disable Bluetooth.
- Delete search history, or use a private browsing mode.
- Do not store sensitive information on your phone.
- Avoid sending sensitive information in messages.
- Delete sensitive messages/photos/videos.
- Never leave your phone unattended.
- Don’t sign into your accounts on someone else's phone.

Avoid carrying these items

if you anticipate physical inspection

- Smartphones
- Smartwatches
- Laptops and Tablets
- GPS Systems

These devices can constitute a security risk, as they can be used to obtain or record your personal information.

Other useful safety measures

Speak in code:

Use simple phrases or signals to convey important messages without drawing attention.

For example, ‘Are you safe?’ could be coded as ‘How's the weather?’ – agree on these codes with your trusted friends beforehand.

Delete sensitive chats:

Regularly clear out risky or compromising conversations to protect your privacy and cover your tracks if needed.

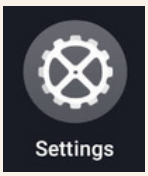
These tips might seem a bit mysterious, but they can be a real lifesaver in tricky situations. Stay one step ahead and keep yourself safe!

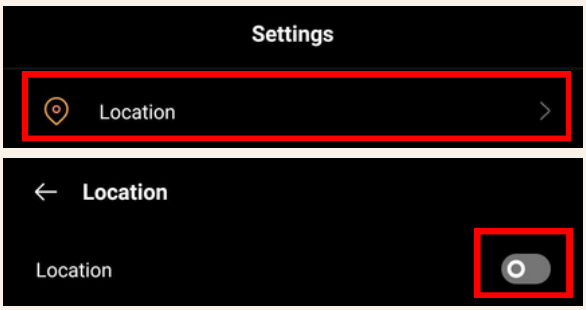
MOBILE DEVICE SECURITY STEPS

Secure your Android

Disable WiFi, GPS location and mobile data:

‘Settings’ → ‘Location.’



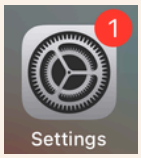


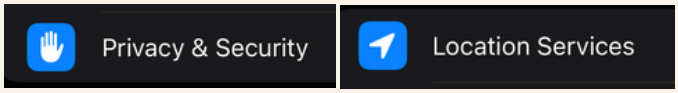
Tap the slider to turn off location.

Secure your iPhone

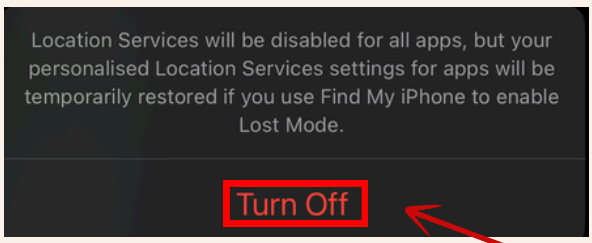
Disable WiFi and GPS location:

‘Settings’ → ‘Privacy & Security’ → ‘Location Services’





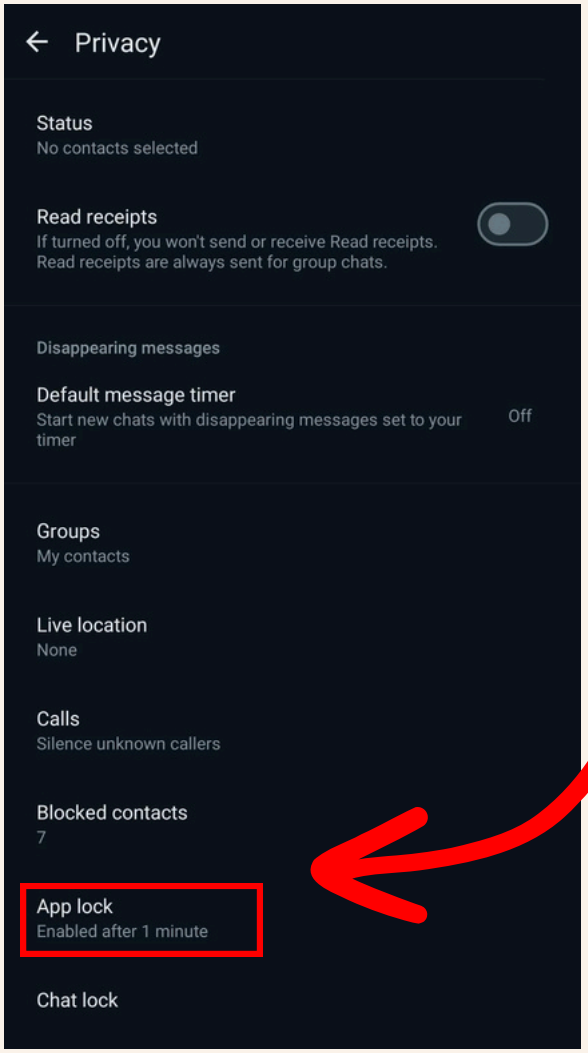
Turn off all ‘Location Services’ using the main slider or the individual sliders for each app



Tap the slider to turn off location.

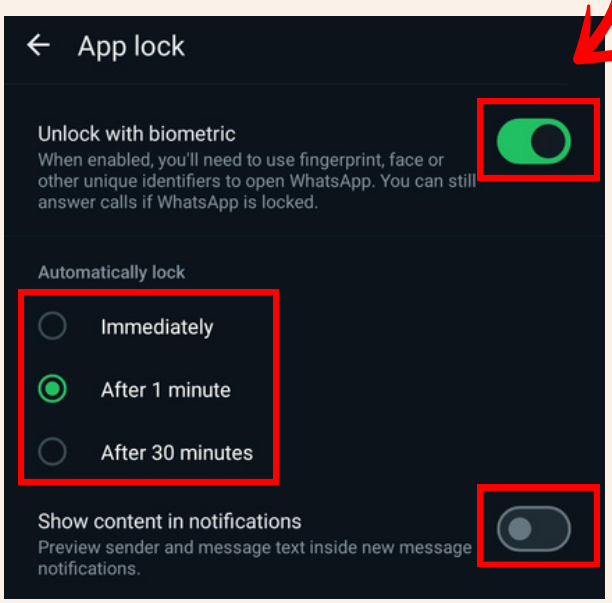
WHATSAPP PRIVACY STEPS

Lock your app



Open WhatsApp 'Settings' → tap 'Privacy' → 'App lock.'

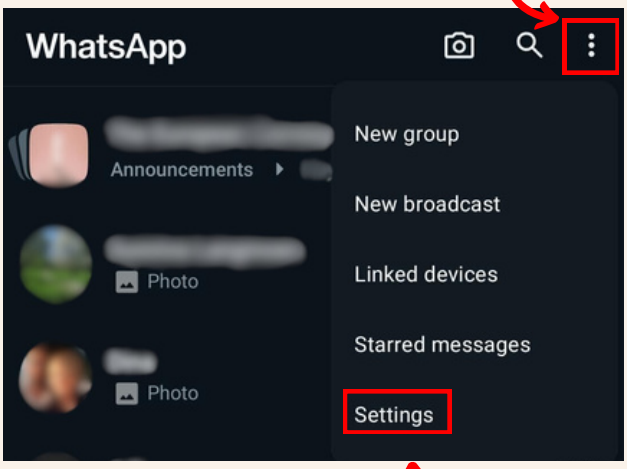
Turn on 'Unlock with biometric' → touch the fingerprint sensor or scan your face to confirm.

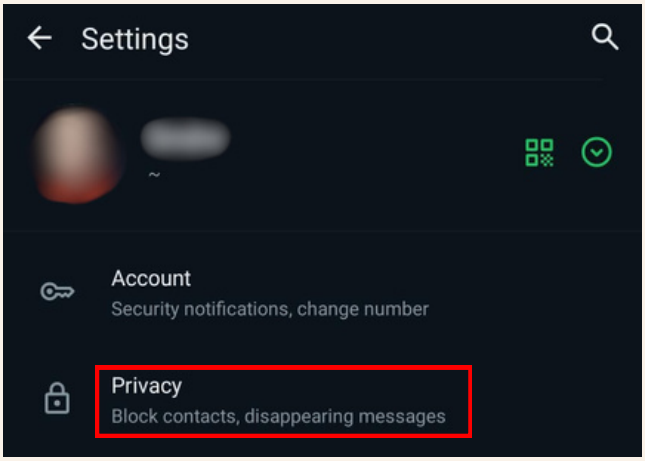


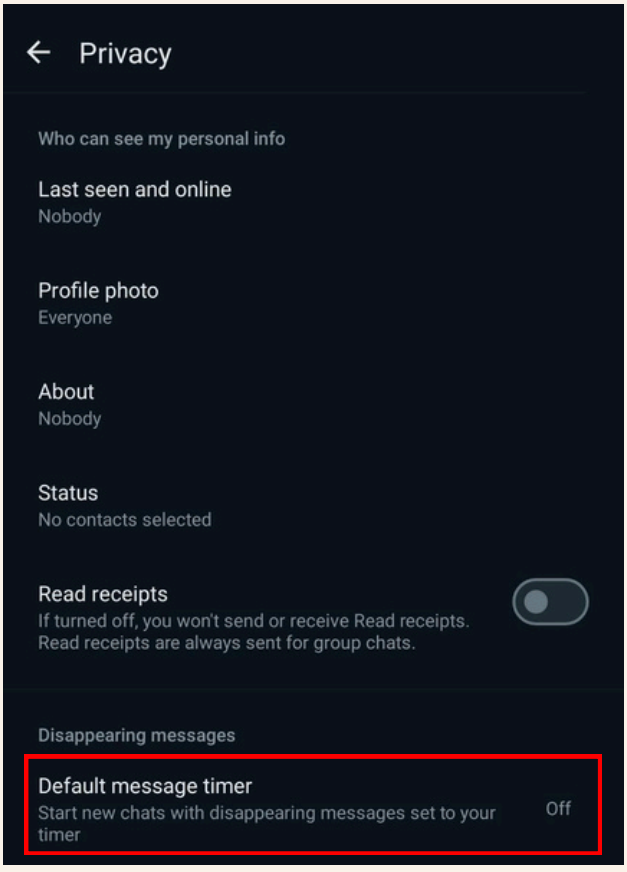
Set the amount of time after which your app is locked and disable 'show content in notifications.'

Turn disappearing messages on or off

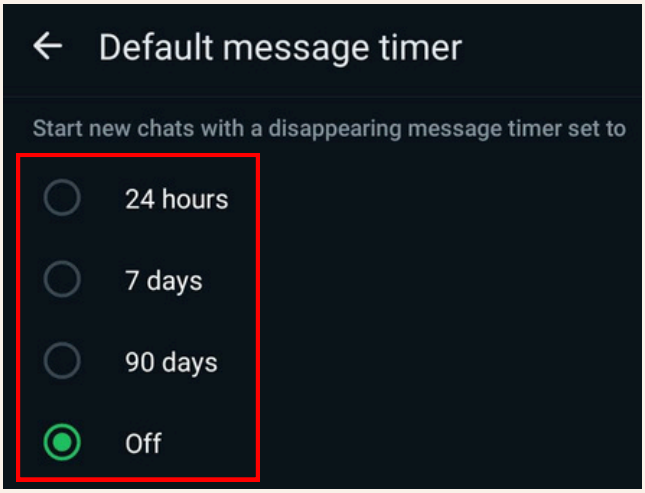
Tap the three dots → ‘Settings’ → ‘Privacy.’







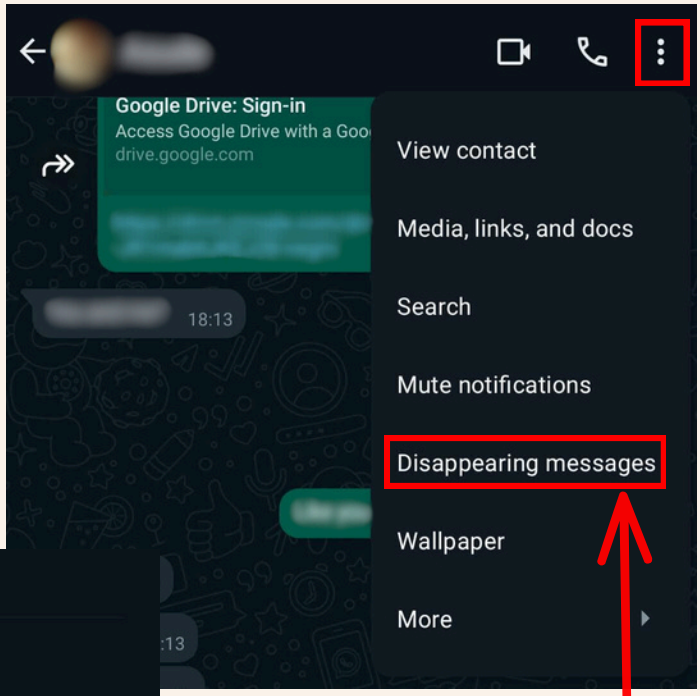
Tap ‘Default message timer.’



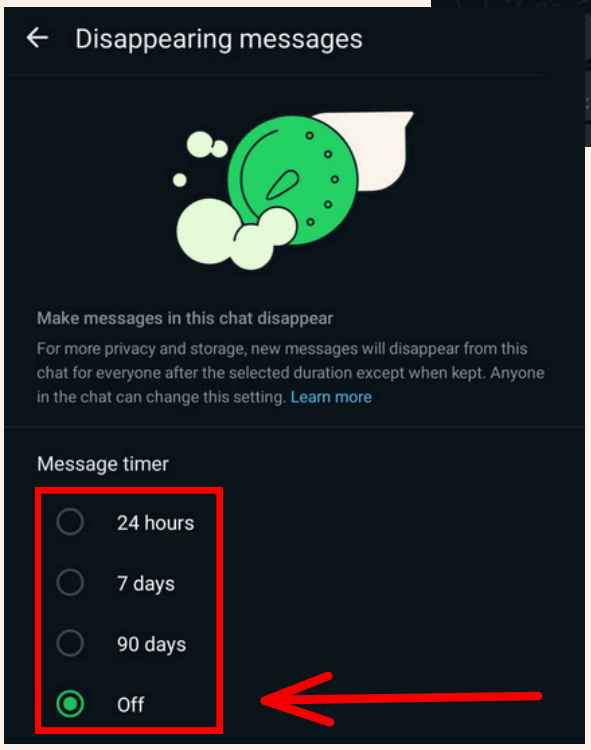
Select 24 hours, 7 days, 90 days, or ‘Off.’

Turn on disappearing messages in an individual chat

Open a chat and tap the contact's name (or the three dots).

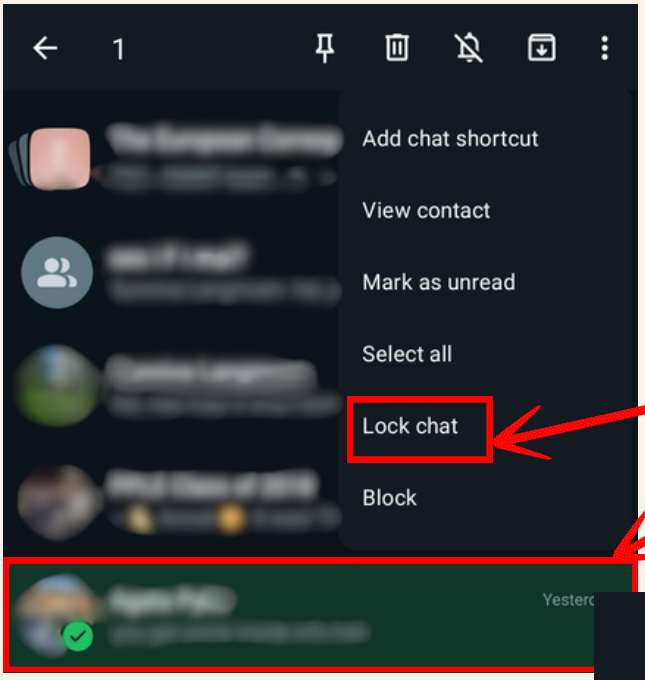


Tap 'Disappearing messages.'



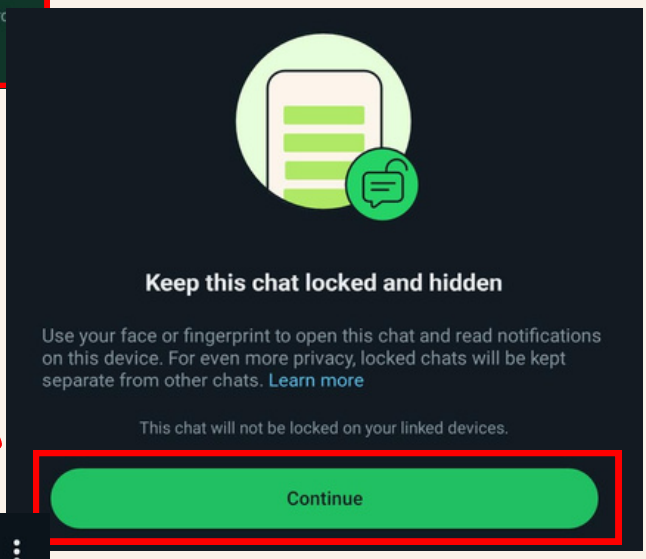
Select 24 hours, 7 days, 90 days, or 'Off.'

Lock your chats

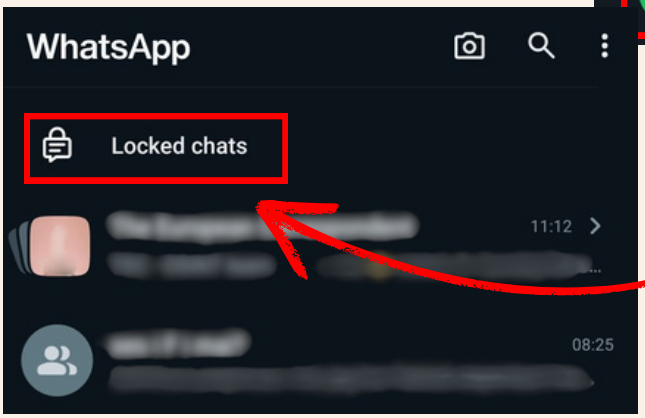


Press and hold on the chat you want to lock.

→ ‘Lock Chat’



→ ‘Continue’
→ ‘Confirm face or fingerprint to lock’

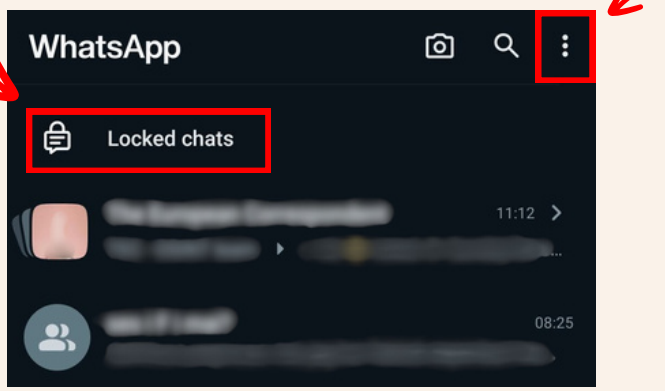


Your chat has now been moved to the ‘Locked chats’ folder!

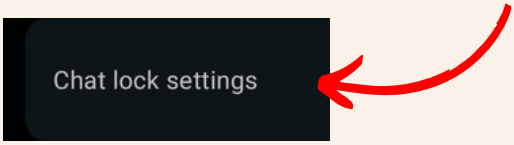
Lock your chats (with secret code)

After turning on the chat lock, you can lock your chats with a different secret code from your phone passcode.

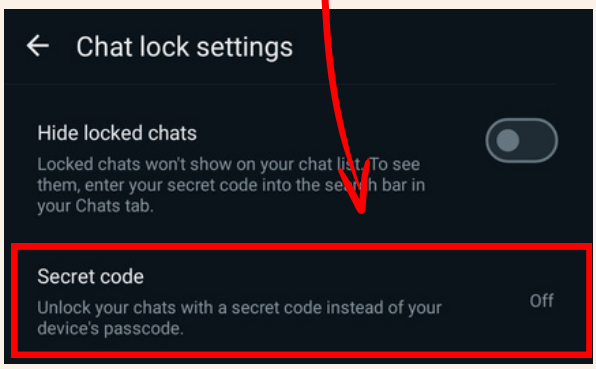
Go to your 'Locked Chats' folder,
→ tap the three dots on the top right



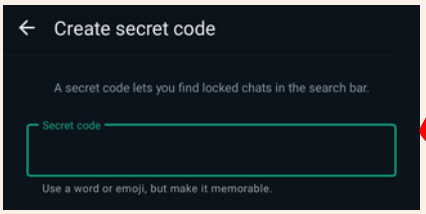
→ Tap 'Chat lock Settings.'



→ Tap 'Secret Code'



→ Create secret code and confirm

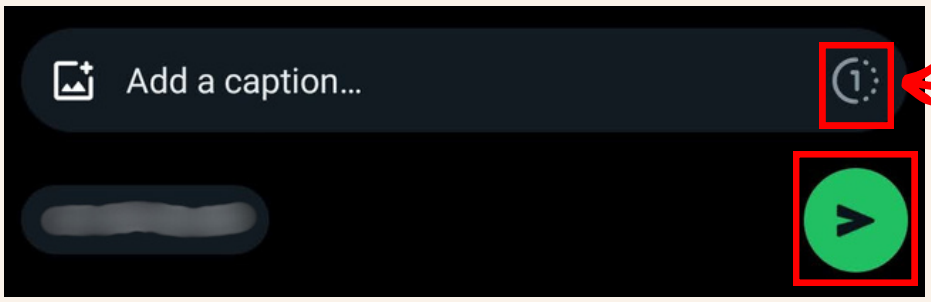


Send One-Time viewable images/videos

Open an individual or group chat.

Select an image or video to send, or take one with the camera.

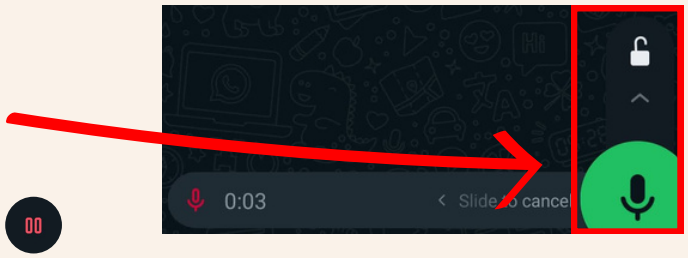
Tap the icon on the bottom right hand corner, then press send!



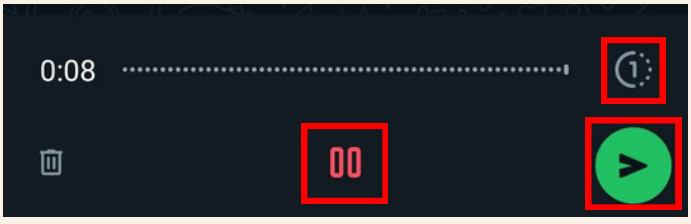
Send One-Time playable voice messages

Open an individual or group chat.

Hold down the microphone on the bottom right corner and swipe up.



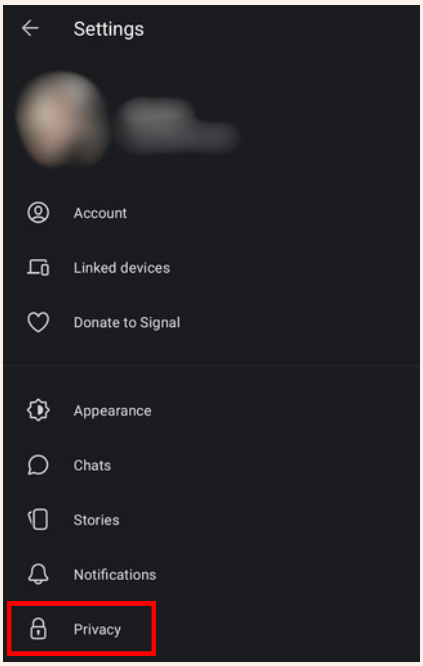
When you are done recording, press → Tap the icon → press send!



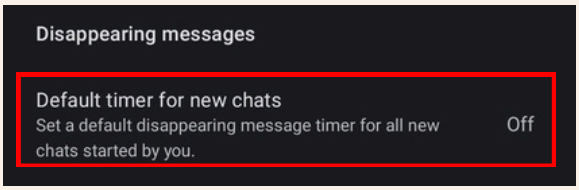
SIGNAL PRIVACY STEPS

Turn disappearing messages on or off

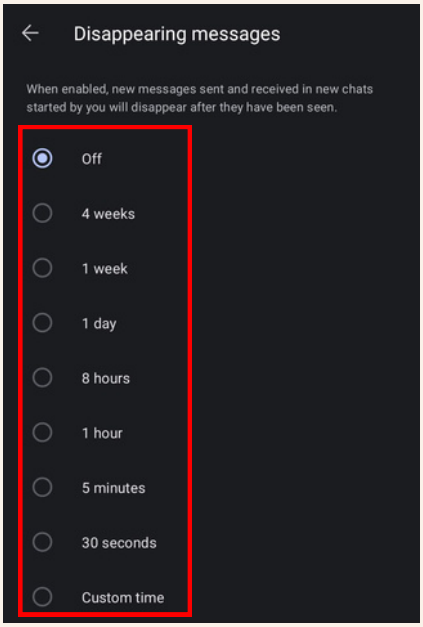
Tap on your profile picture → 'Privacy.'



Scroll down to 'Disappearing Messages' and tap 'Default timer for new chats.'

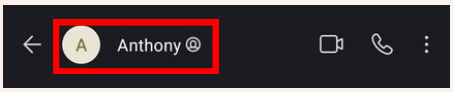


Select your preferred amount of time before messages disappear.

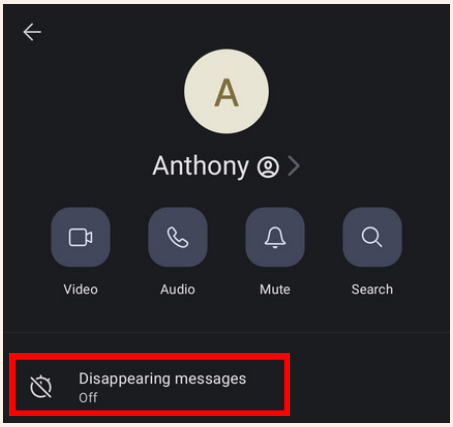


Turn on disappearing messages in an individual chat

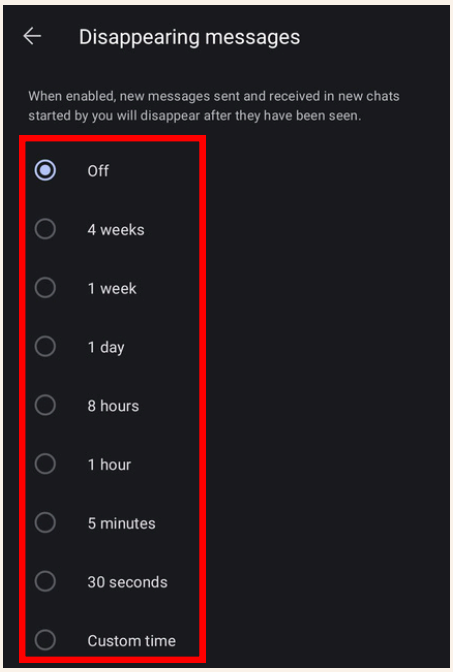
Open a chat and tap the contact's name.



Tap 'Disappearing messages.'

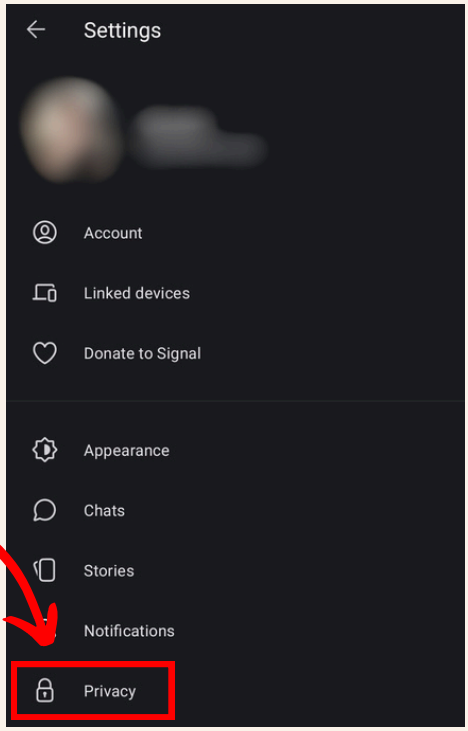


Select your preferred amount of time before messages disappear.

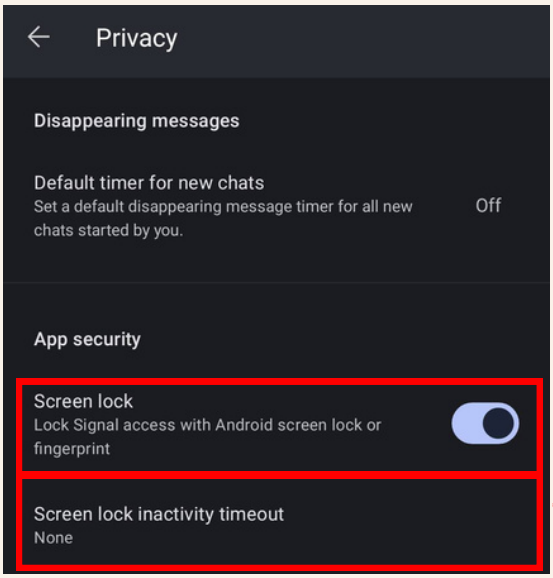


Lock your Signal

Tap on your profile picture → ‘Privacy.’



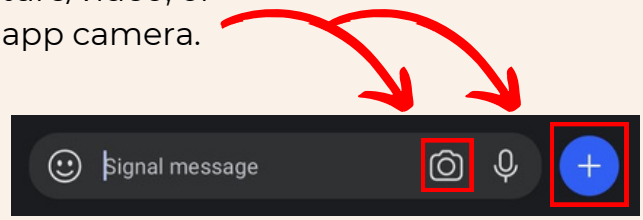
Under ‘App Security,’ toggle the button ‘Screen Lock.’



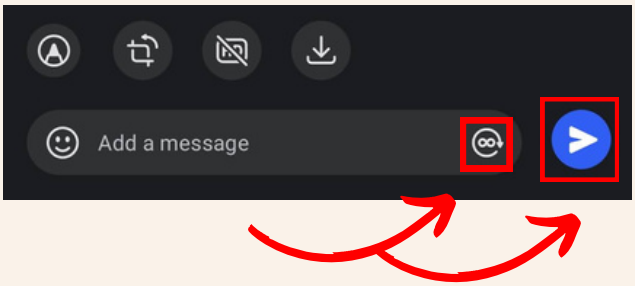
Press ‘Screen lock inactivity timeout’ to select the time duration after which your Signal app will be locked.

Send disappearing pictures/videos

Open a chat and choose a picture/video, or take a picture/video from the app camera.

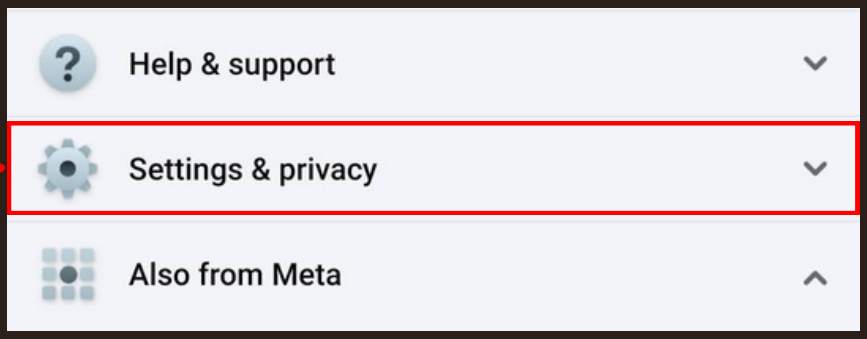


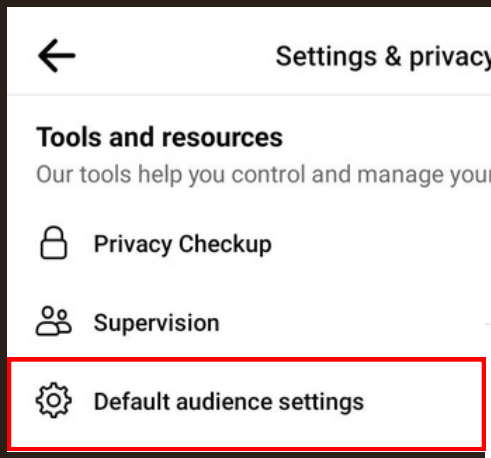
Tap the icon on the bottom right hand corner, then press send!



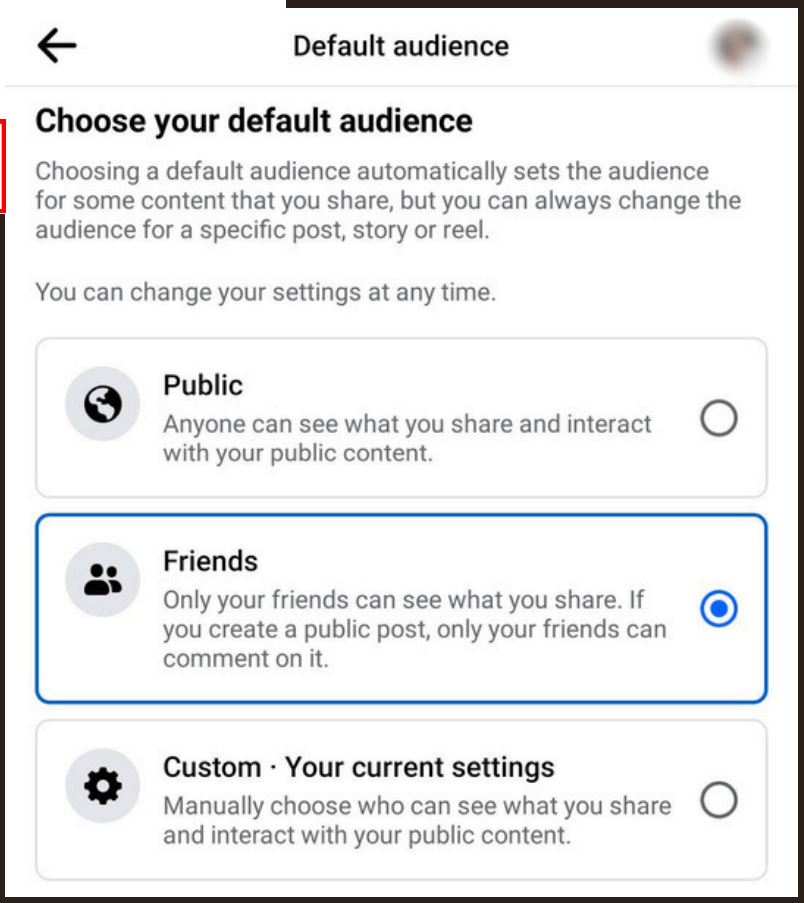
03. SECURING SOCIAL MEDIA

FACEBOOK PRIVACY STEPS

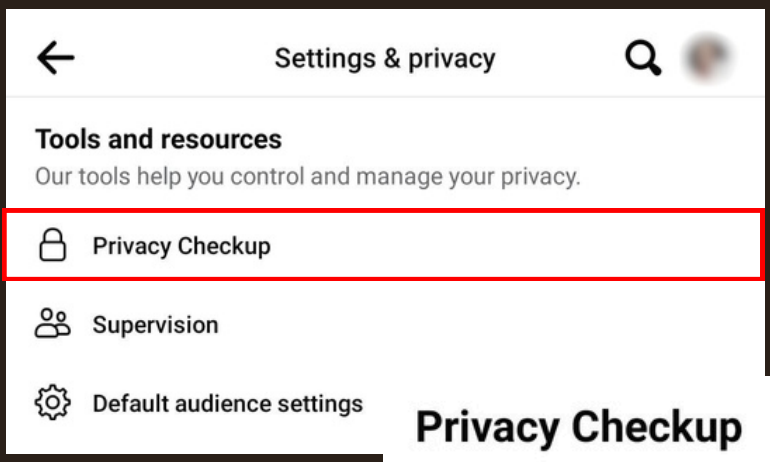


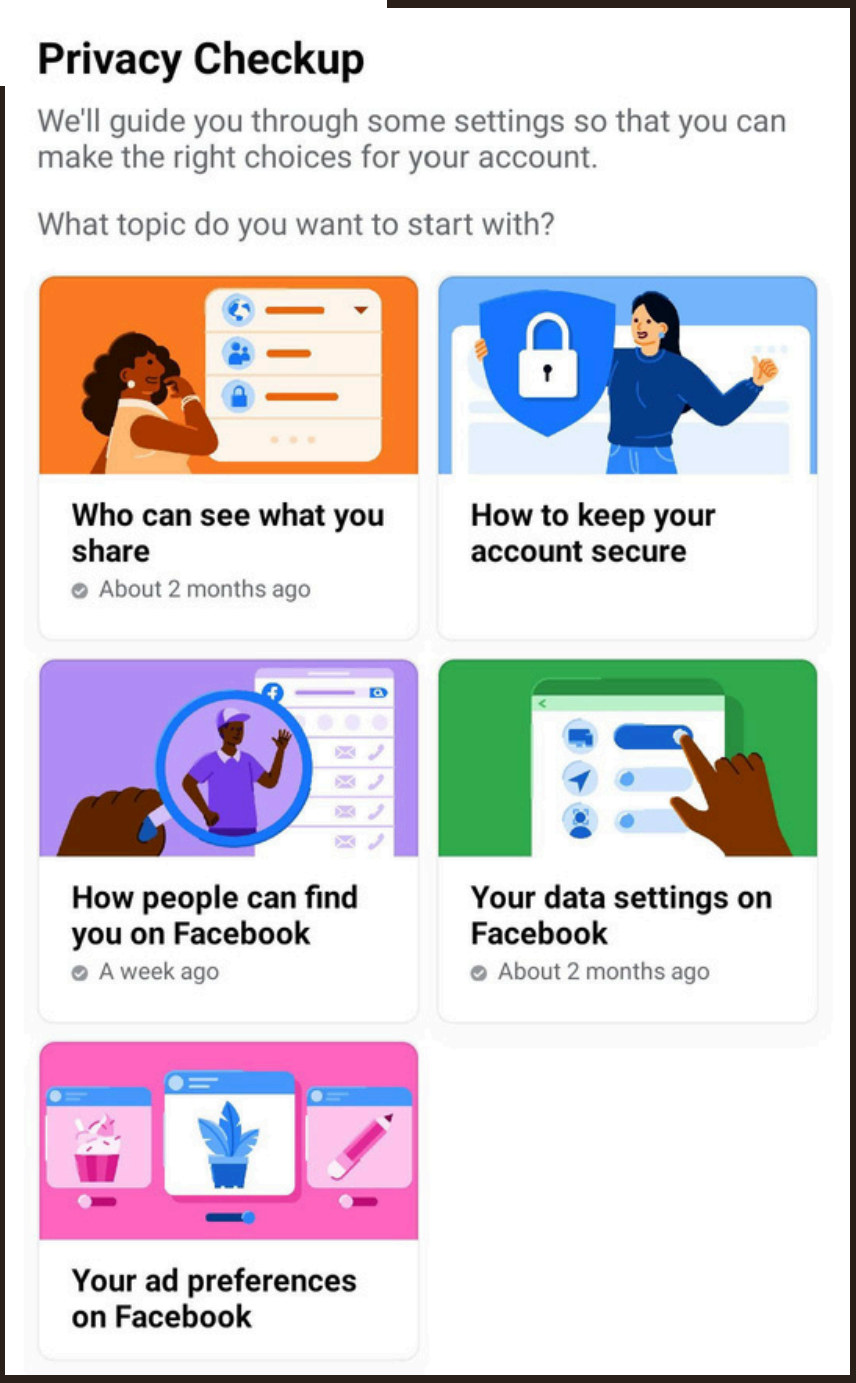


The ‘Default audience settings’ tab lets you decide who can see your posts and stories, and more.

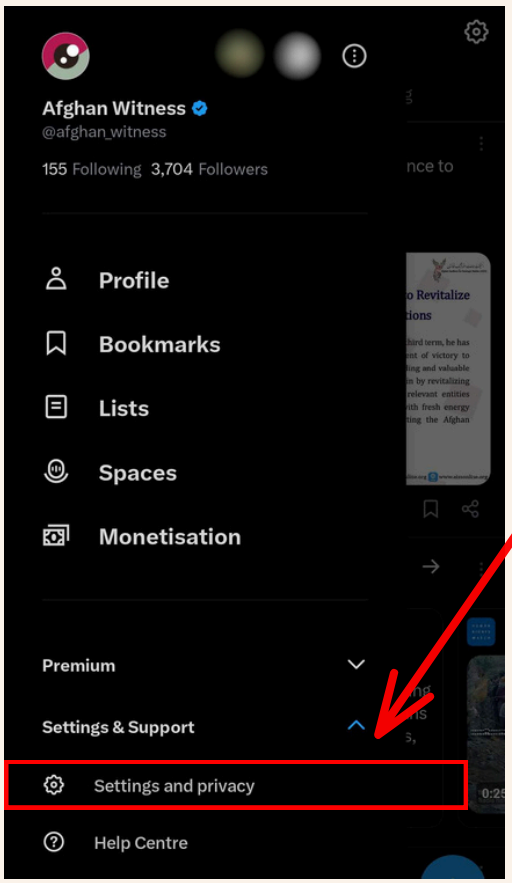


The ‘Privacy Checkup’ tab provides you with more detailed settings, enabling you to maximise privacy settings.

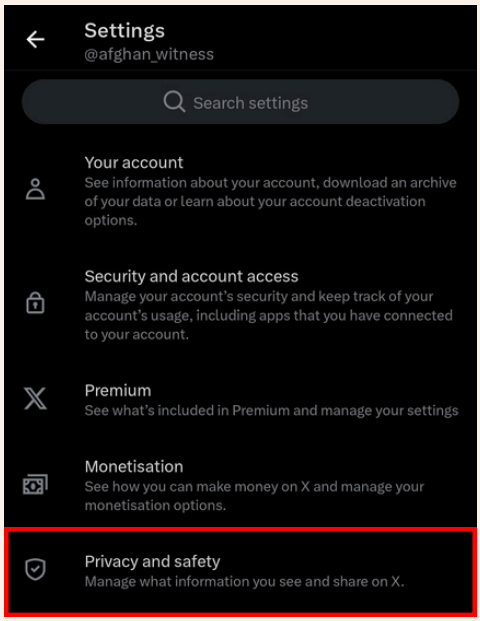




TWITTER/X PRIVACY STEPS

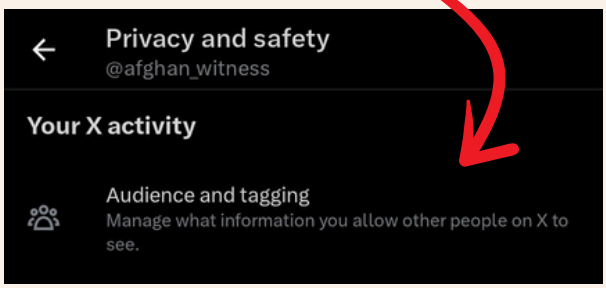


Press your profile picture, tap ‘Settings & Support’ and then ‘Settings and privacy.’

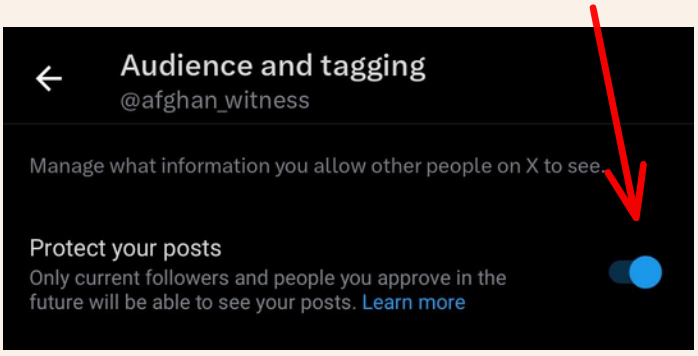


Now, click on ‘Privacy and safety.’

Now press ‘Audience and tagging.’



Check ‘Protect your posts’ so that only your followers are able to see your posts.

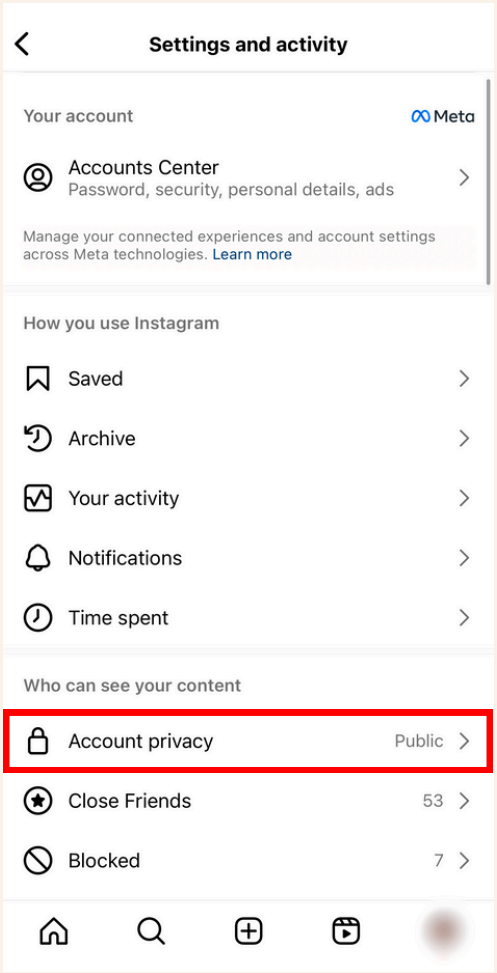


INSTAGRAM PRIVACY STEPS

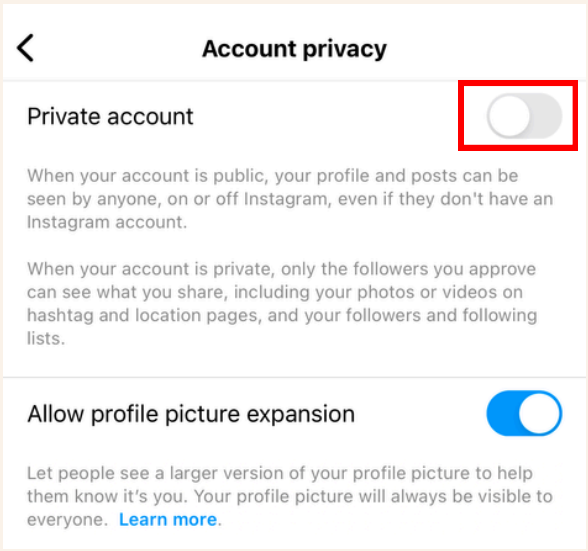
Tap on your profile picture in the bottom right.

Now, tap the three bars in the top right corner.

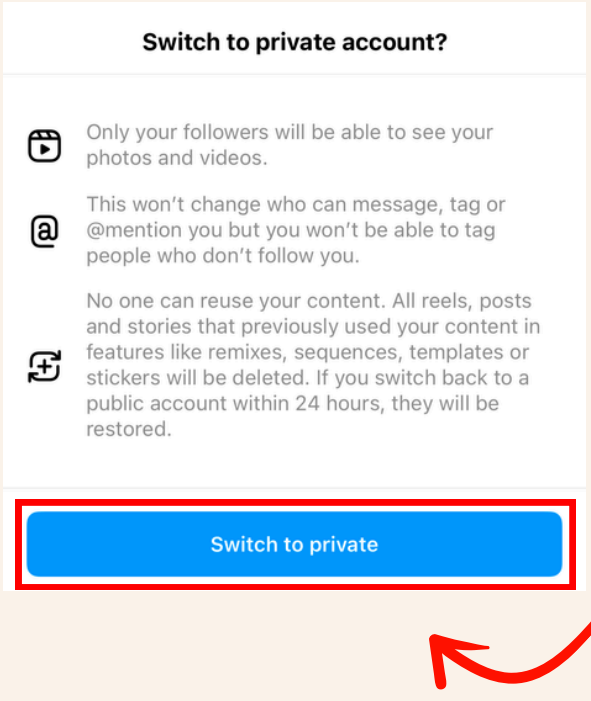
Below ‘Who can see your content’, tap ‘Account privacy.’



Slide where it says ‘Private account’ to make your account private.



Tap ‘Switch to private’ to confirm.



04. BROWSING THE WEB

UNDERSTANDING THE DANGERS

When you browse the web, you expose yourself to various risks.

You may be subjected to **tracking** and **surveillance** by authorities or even family members, who can gain access to your entire internet traffic.

You may risk being the target of **malware attacks**, where your devices are infected by software that steals your data and observes your activities.

You may be the target of a **phishing attack**, which is when an attacker attempts to deceive you into providing information such as usernames, passwords or financial details, by using fake messages, emails or websites designed to trick you into believing they are legitimate.

You may also become the victim of a **data leak**, which is when otherwise trustworthy services are hacked and their data is stolen – data which may contain your personal information.

By taking certain precautions, you can **minimise your vulnerability** to these attacks.

VPNS AND ANONYMOUS BROWSING

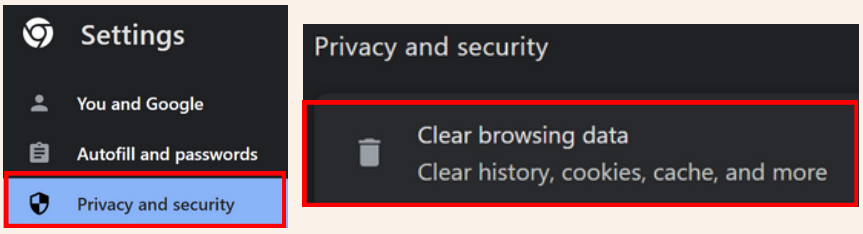
Virtual Private Networks (VPNs) hide your IP address and encrypt your connection, making it very difficult for anyone observing the internet activity coming from your device or from your home to monitor you. Choose a reputable VPN service. While most VPN services have a monthly fee, Proton VPN has a great free option.

For greater protection, the **Tor Browser** uses a special decentralised encrypted network which is not under any government's control, and is free. The browser gives you the greatest anonymity online. However, you should avoid logging into your personal accounts using Tor.

Erase your browser history

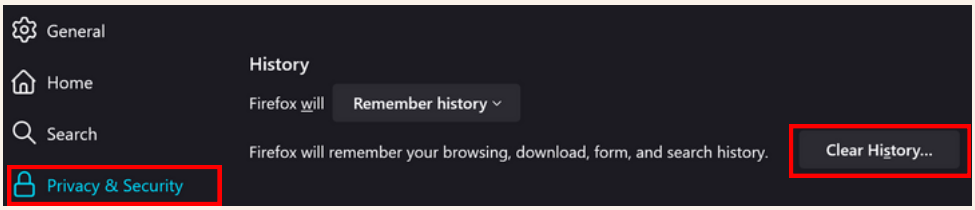
Chrome

‘Settings’ → ‘Privacy and security’ → ‘Clear browsing data’



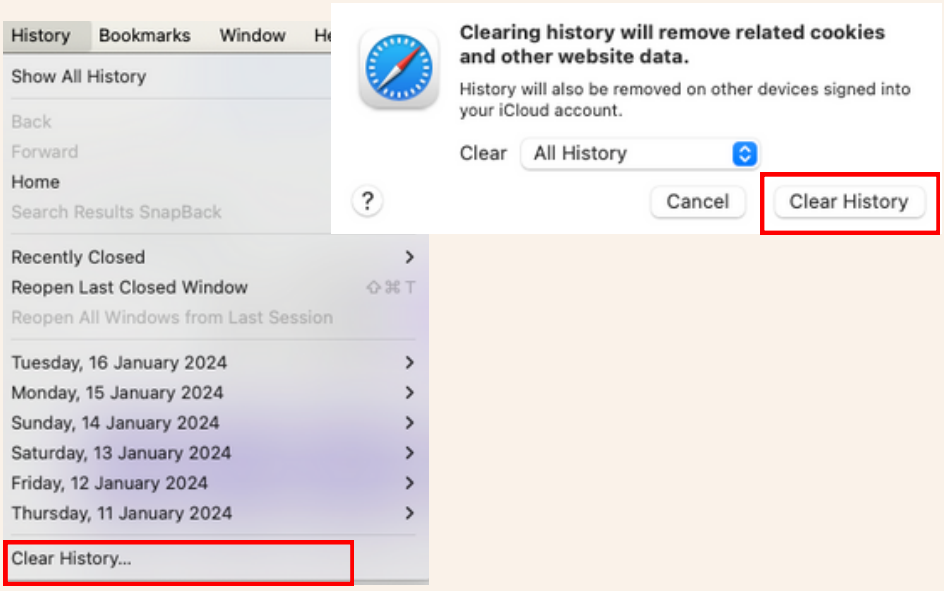
Firefox

‘Settings’ → ‘Privacy & Security’ → ‘History’



Safari

‘Settings’ → ‘Safari’ → ‘Clear History and Website Data’



Use private browsing

Use the following shortcuts to use private browsing:

Chrome — Ctrl + Shift + N

Firefox — Ctrl + Shift + P

Safari — Command + Shift + N

Private browsing mode is a feature in web browsers that **prevents the storage of history, cookies, and other local data** from your browsing session, helping to protect your privacy.

It does **nothing** against anyone observing your online activities from the **outside**, however, by anyone with access to your network – so you should take other precautions.

Use a VPN (Virtual Private Network)

A VPN, or a Virtual Private Network, is a way of **disguising your IP** and **encrypting** all of your internet traffic so that no one can find out what you're viewing online.

Recommended VPN services:

- Proton VPN (free)
- Tunnelbear (2GB free)
- Surfshark ($2.49 per month)
- NordVPN ($3.99 per month)
- Private Internet Access ($3.33 per month)

Use PC Cleaning software

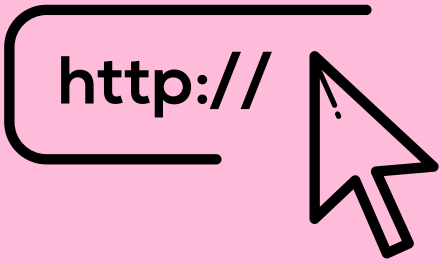
Recommended Free PC Cleaners:

CCleaner

BleachBit

PC cleaning software such as **CCleaner** and **BleachBit** help clean up your computer, optimise performance, and maintain privacy by automatically deleting your history and trash.

Alternative browsers and search engines



For better privacy,
do **not** use **Chrome**, **Safari** or **Edge**,
and avoid the **Google** search engine.

Firefox is a good option, provided you configure it correctly and install some extensions to protect your privacy.

Recommended browsers and engines:

Brave → browser that blocks ads and trackers

Tor → anonymising browser using encrypted network

DuckDuckGo → private search engine

Startpage → private search engine

Browser Extensions

Browser extensions, also known as **add-ons** or **plugins**, are programs that enhance or customise a web browser.

They can help protect your privacy by **blocking third parties** from **tracking your online activity**. However, be cautious as some extensions can be harmful.

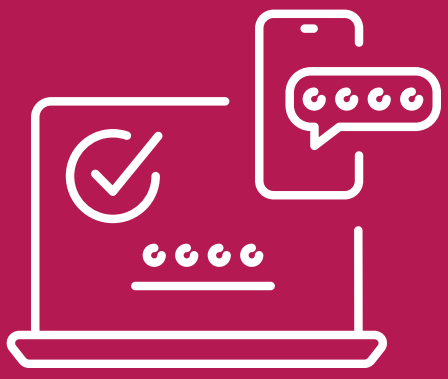
We recommend installing **uBlock Origin**, which will not only block ads and improve your browsing session, but also increase your privacy and make it more difficult for you to be tracked.

05. PASSWORD SECURITY

Password security is **essential for maintaining personal safety** and privacy.

Unfortunately, many people use weak passwords like '123456,' 'password,' or names and birthdates, which are easy to guess and compromise. Some people also store their passwords in their notes, or on a file on their device, readily accessible to anyone who finds it. Others use the same password across all their accounts.

Implementing robust password security helps protect sensitive information and ensures that personal communications, locations, and activities remain private. Using **a password manager is the best way to maximise your security**: it automatically generates secure passwords for all your accounts, while you only need to remember a single one to access them all.



Good practices:

✅ Use at least **15 characters**.

✅ Think of a **passphrase** instead of a password:

A **sentence** or a **collection of random words** makes for an almost unbreakable password, while remaining easy to remember.

Try something like '**smallfrogsittinginatree**' or completely random like '**frozentreeimperfectball**.'

✅ Mixing upper and lowercase letters, numbers, and symbols can improve security – but is unnecessary if your password is long and random enough.

✅ **Test your password strength** with a tool such as www.passwordmonster.com.

✅ **Change passwords** every 3-9 months or as needed.

✅ Use **different passwords** for different accounts.

✅ Use a **password manager**.

✅ Enable **Two-Factor Authentication (2FA)** on your accounts. Mobile apps like Google Authenticator also work very well!

Bad practices:

🚫 Never **re-use** passwords.

🚫 Don't let your **browser save passwords**.

🚫 Don't include any **personal information** in your passwords (e.g. birthday, maiden or pet name, etc.).

🚫 Don't store your list of passwords on your computer in **plain text**.

🚫 Don't store your list of passwords on a **physical piece of paper**.

Password Managers

Password managers generate and store strong, unique passwords, making digital security easier. They keep passwords in a secure 'vault' and protect them with a master password. Benefits include password generation, storage, and autofill across devices.

Their weakness, of course, is that they are a single point of failure. If someone gains access to your password manager, they have access to all your login information to all your accounts.

It is crucial that you choose a strong master password for your password manager and that you ensure that your device is protected against malware. Enable two-factor authentication when possible.

KeePass is a free, open source and easy-to-use password manager, which does not depend on any web services to function.

After creating your password database and your master password, you can keep your database file on your computer, on your phone, or you can place it on a cloud platform such as Google Drive, so you may access it anytime and anywhere. It is the more manual choice, giving you greater control but also greater responsibility to manually update the program and keeping the database file safe.

It also features apps for Android and for iOS.

BitWarden has both paid and free options. It is a more user friendly option than KeePass, and your passwords are immediately backed up into the cloud, without you having to manage the database yourself as with KeePass. It also automatically updates. It is a more convenient choice than KeePass.

It also features options for Android and iOS.

06. PHYSICAL SECURITY

SAFEGUARDING PERSONAL DEVICES

Keep devices hidden: Always keep your phone, laptop, or tablet out of sight when not in use, especially in public places. This reduces the risk of theft or confiscation.

Enable device encryption: Use device encryption features to protect your data. This ensures that if your device is lost or stolen, the data cannot be accessed without the correct password. It is enabled by default in later models.

DEVICE LOSS

If your device is lost or stolen, you can wipe its content remotely by using Find My Device (also on iPhone).

In order to avoid losing your data if you lose your device, make sure to regularly back up important data to a secure cloud service or an encrypted external drive.

SAFE PRACTICES ONLINE

Avoid sharing your location in real-time on social media. Be mindful of posting details that could reveal your whereabouts, and make sure to have maximised your account's privacy settings.

RECOGNISING PHYSICAL SURVEILLANCE

Be alert to unfamiliar individuals who seem to follow or watch you. Change your routines to avoid predictability.

If you suspect that you are being followed:

- **Do not** go straight home, do not make direct eye contact with the person, or run directly to your destination.
- **Observe**: Stop at a shop window and use peripheral vision, quick glances, or reflections to observe the person following you. Make mental notes of their appearance and behaviour.
- **Stay on public streets**: Continue walking on public streets, move into crowds where possible, and take the next available turn to change direction. Repeat steps until you have lost your pursuer.
- **Recognise patterns**: Keep in mind that one-time occurrences are normal, two times may be coincidental, but three or more times indicates a potential threat.

Emergency Routines

Establishing **emergency routines** can significantly enhance your safety and provide peace of mind to you and your trusted contacts.

Here are some effective practices you can implement:

Let trusted people know your plans

Share your itinerary:

- Before you leave: Always inform a trusted person about your travel plans, including your destination, route, and expected time of arrival.
- Daily plans: Share your daily schedule, especially when attending meetings or visiting unfamiliar places.

Regular check-ins:

- Scheduled check-ins: Agree on specific times to check in with your trusted contact. This could be through a quick phone call, text message, or social media update.
- Code words: Use predetermined code words or phrases to confirm your safety or signal distress without raising suspicion. For example, a phrase like "I'm with Aunt Sara" could indicate that everything is fine, while "I'm going to visit my cousin" might signal you are in trouble.

Emergency signals and alarm protocols

Missed check-ins:

- Immediate action: If you miss a scheduled check-in, your contact should try to reach you through all available means (phone calls, messages, etc.).
- Alarm activation: If they cannot reach you within a predetermined time frame, they should alert trusted relevant authorities or other designated emergency contacts. Agree on this process beforehand.

Distress signals:

- Silent alarms: Use subtle signals if you need help but cannot speak freely. This could be sending an agreed-upon emoji or a code message.
- Call for help: If in danger, call your trusted contact and let the phone remain connected, even if you can't speak. This allows your contact to hear what is happening and take necessary action.

WHEN TRAVELLING OR CROSSING BORDERS

UNDERSTANDING THE DANGERS

When travelling, particularly when crossing borders, security agents may often freely search your electronic devices, potentially exposing your sensitive data. They may confiscate your devices, and the data contained therein may be copied and scrutinised. They may access your personal photos, contacts and communications, which may put not only yourself, but also others, in danger.

By taking important precautions, you may secure yourself against such intrusion.

PREPARATION BEFORE TRAVEL

Carry a 'clean' device: delete all unnecessary files, ideally using a secure deletion tool. **Ensure that data and files do not remain in your junk folder.**

Log out of personal accounts, remove saved login credentials, clear all your cached data, and uninstall any sensitive apps.

Back up your data to a secure place, either to a cloud service that is not connected to your device, or to a different drive or device. This will help you restore your data once you are in safety, or enable you to recover your data if your device is lost or confiscated.

Create temporary email and social media accounts for use while travelling, decreasing suspicion while hiding your personal accounts.

If possible, travel with a temporary phone or laptop, to which you have transferred only essential and safe information.

Be careful that your device is not so clean that it is suspicious – you want your phone to look normal, containing some photos, text messages and apps.

AFTER TRAVELLING OR CROSSING A BORDER

Inspect your devices for signs of tampering, such as unfamiliar apps or altered settings. **If you suspect tampering, consider wiping and restoring the device from a backup.**

Change the passwords for any accounts accessed during travel. This mitigates the risk if your passwords were compromised.

When you are in security and have access to the internet, you may then restore your data from your backups.

ADDITIONAL RESOURCES

LINKS

Access Now — Guide to Safer Travel (English)

Chayn — Advanced DIY Privacy for Every Woman (English)

Chayn — DIY Online Safety (Farsi)

CiviCert — The Digital First Aid Kit (Farsi)

EFF — Surveillance Self-Defense guide (English)

EFF — Street-Level Surveillance project (English)

Freedom of the Press Foundation — Secure communication (English)

Human Rights First — Steps to Protect Your Online Identity from the Taliban: Digital History and Evading Biometrics Abuses (Farsi & Pashto)

Privacy Guides — Knowledge Base (English)

Tactical Tech — Resources (English)

The New Oil — The Beginner's Guide to Data Privacy & Cybersecurity (English)

DEFINITIONS

Encryption: Turning information into a secret code so only people with the key can read it, keeping it safe from others.

End-to-End Encryption: A way to send messages so that only the sender and the receiver can read them, making sure no one else can see the information.

Open-Source: Software that anyone can look at, use, modify, and share. It is often created by a community of developers.

Firewall: A security tool that blocks harmful internet traffic from getting into your computer or network, acting like a barrier to protect your data.

Antivirus: A program that finds, removes, and protects against harmful software (viruses) that can damage your computer or steal your information.

Malware: Any software that is designed to harm your computer or steal your data, including viruses, spyware, and ransomware.

Phishing Attack: A specific type of scam where fake messages try to trick you into giving away your personal details, often by pretending to be from a trusted company or person.

Social Engineering: Manipulating people into giving up confidential information by pretending to be trustworthy or using psychological tricks.

VPN (Virtual Private Network): A service that creates a secure and private connection over the internet, hiding your online activities and protecting your data from spying.

Two-Factor Authentication (2FA): An extra layer of security for logging into accounts, requiring not just a password but also something else, like a code sent to your phone.

Passcode: A series of numbers or letters that you use to unlock your phone, computer, or apps, helping to keep your information secure.

Password Manager: Software that creates, stores, and manages your passwords securely, so you only need to remember one main password.

DEFINITIONS

Tracking Cookies: Small files that websites save on your computer to remember your actions and preferences, often used to track your browsing habits for advertising.

Private Browsing Mode: A feature in web browsers that doesn't save your history, cookies, or search records, helping to keep your browsing private.

Biometric Information: Data based on physical characteristics like fingerprints, facial recognition, or iris scans, used to identify and verify people.

Adblocker: A tool or browser extension that prevents advertisements from appearing on the websites you visit, making your browsing experience cleaner and faster.

PC Cleaning Software: Programs like CCleaner and BleachBit that clean up your computer, improve performance, and maintain privacy by deleting history and unnecessary files.

Tor Browser: A special web browser that hides your online activity by bouncing your connection through multiple servers, making it hard for anyone to trace what you do online.

GPS Location: A system that uses satellites to find and show your exact location on a map, useful for navigation and location-based services.

Bluetooth: A technology that allows devices like phones, headphones, and computers to connect and share information wirelessly over short distances.

Secure Messaging Apps: Apps like Signal or WhatsApp that use strong encryption to protect your messages so that only you and the person you're talking to can read them.

Data Leak: When private information is accidentally or deliberately exposed, making it available to people who shouldn't have access to it.

Browser Extensions: Small software programs that you can add to your web browser to give it more features, like blocking ads or translating languages.

#WOMENSAFEONLINE

afghanwitness.org

@afghan_witness

@AfghanWitnessOfficial

@afghan_witness