App protection and settings

Note: Detailed explanations are indicative, and may change with operating system and software updates. Android functionality varies according to the device manufacturer.

How can I prevent my abuser or stalker from monitoring my private messages?

See *Safeguarding Devices* for how to prevent unauthorised access to your mobile phone or tablet.

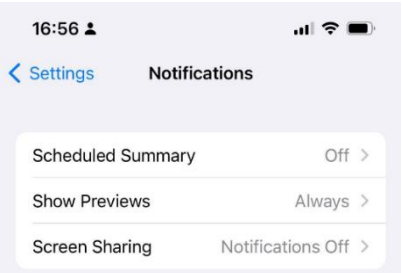
You can change how message notifications are displayed (whether the device is locked or unlocked), and what sounds are played, or even turn off notifications altogether. Setting your phone or tablet to silent will help to hide any notifications you receive. For phones, using vibration alerts will ensure you know you have received a message - however, in a very quiet environment, or if the phone is placed on a hard surface, other people can hear a vibration alert.

App settings

Most apps, as well as in-built messaging functions (e.g. Apple iMessage), have notification settings specific to the app. These can be found on an iPhone via Settings then the individual function or app (e.g. Change message notification on iPhone for iMessage); and on Android via Settings > Notifications > App settings.

This is a useful way to keep messages hidden from an abuser, but may mean that you miss messages yourself.

Message preview



Notification settings on an iPhone

When notification preview is switched on, all or some of a message can be seen on the lock screen of your device. An abuser with access to your device will not need to unlock it to see the message.

On an iPhone this can be turned off for all apps and functions via Settings > Notifications > Show Previews.

For Android devices the setting is slightly different - you can turn off sensitive content in notifications. This will work across all apps, so long as the app developer has set the content to count as 'sensitive'.

For both iPhone and Android if you use these settings the notification will appear on the lock screen, but no content will be visible unless you unlock the device. If an abuser has access to your device they will be able to see that you are receiving notifications, but will not be able to see the content - this may make them suspicious.

Multiple devices

If you use more than one device you will need to adjust the settings on each device. If you can identify apps via which you might receive sensitive messages, it will help to keep those apps on one device only. For example, log into Facebook only on your phone, and not your tablet. Ideally you would use the device you are best able to keep under your own control - typically a phone rather than a tablet.

Two step verification/two factor authentication

Two step verification (2SV) or two factor authentication (2FA) are ways to add extra protection to accounts. Apply 2SV/2FA to all your accounts that offer it. Depending on the app or account, this may:

- Alert you to attempts to access the account, e.g. WhatsApp 2SV requires a code before the account is set up on a different device.
- Prevent certain activities happening, e.g. payments being made.
- Help to build evidence against an abuser.

2SV/2FA is currently most often delivered by SMS, although other methods, including email and authentication apps, may also be used. If you are in the same place as the abuser, the arrival of an SMS or other notification may make them realise you are using 2SV/2FA on the account. If this is a possibility, you may want to turn off notifications.

In a domestic abuse situation, forms of 2SV/2FA that are only delivered to a single designated device are the best option - authenticator app, or SMS. Other methods, e.g. email, might be accessible on another device, and therefore to the abuser.

2SV/2FA messages sent by SMS may be intercepted if the abuser has access to the phone being used. See:

- **Message preview** in this handout for how to prevent the code being visible on the phone's lock screen
- **Using a SIM PIN** in the **Safeguarding Devices** handout for how to prevent the SIM being used in another phone

2SV/2FA in evidence

Using 2SV/2FA may help to build evidence against an abuser by demonstrating that they are committing Computer Misuse Act Offences. (CMA Section 1 legislates against unauthorised access to computer material) as well as potentially other Domestic Abuse offences.

It will be difficult to prove unauthorised access if you have shared PINs or passwords with an abuser. Proof would be needed if this was done through violence or coercion.

Login attempt notifications will show time and date of attempts, location, device. This is not wholly accurate but could be used as intelligence.

If the device you are using belongs to the abuser then their unauthorised access to the device may be difficult to prove. CMA offences may apply if the abuser repeatedly tries to access any of your devices or accounts without permission.

Deleting messages, photos and videos

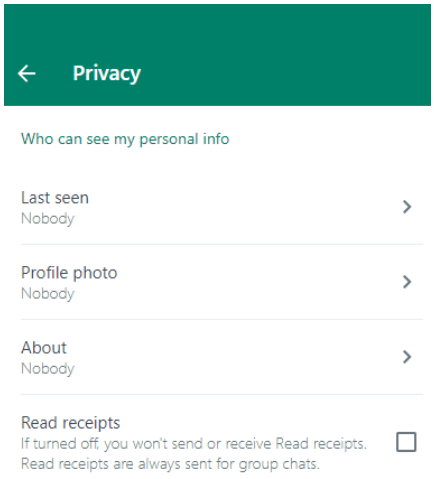
When you delete photos or videos from the main photo area (Photos on iPhone; Google Photos, Photo Gallery, Gallery or similar on Android) they will remain in the Recently Deleted folder/Recycle Bin for 30 days. You can delete them from Recently Deleted/Recycle Bin to make sure they are fully deleted from your device.

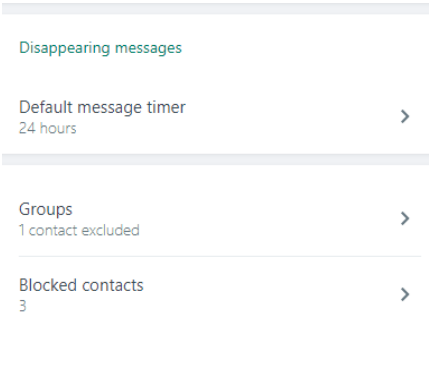
If you delete a message, photo or video from a chain of messages, e.g. in iMessenger or WhatsApp it may leave a box showing a message/photo was removed. You may be able to remove this box itself, leaving no sign that anything has been deleted.

If you need ensure that a photo or video cannot be accessed on your device at all, you will need to remove it from any app in which you've shared it, from Photos/Gallery, and from Recently Deleted/Recycle Bin.

In a situation where the abuser has access to the device and/or messages, you should be aware that deleted messages might appear suspicious - for example if there is a long pause in a conversation which is usually very active, a conversation doesn't make sense because of the missing messages, or the abuser knows the conversation took place but can see no evidence of it on the device.

Messaging app settings





Messaging apps have a variety of settings offering different degrees of security and privacy.

This can include:

- Who sees your profile information and/or picture
- Who can see if you are currently online, or when you last were

- Whether you send and receive 'read' receipts
- Who can add you to groups
- Disappearing messages

This is specific to apps, and if you need to be secure in your messaging, you will need to be aware of what your app offers.

As an example, these WhatsApp privacy settings mean:

- No one when they last were (however it will show if they are currently online)
- No one can see their profile photo or about information
- No one can see when they have read messages
- In any individual chats (not groups) started after the message timer setting was changed, their messages will delete after 24 hours
- They can be added to a group by all their contacts bar one named person
- They have blocked three contacts

These are fairly secure settings, but will not guard against an abuser having access to the phone, or any other linked device. WhatsApp can be accessed on up to four devices in addition to the original phone (access to the original phone is needed to set this up). You can check what devices are able to access your WhatsApp via Settings - Linked Devices, and you can remove access (Log Out) from any devices you do not recognise.

For any messaging app you use, you should get to know the settings, how they can help you stay safe, and how they might leave you vulnerable.

Disappearing messages

This facility in WhatsApp can be useful, but does have some potential pitfalls:

- Setting your default (as above) to disappearing messages will only apply to new individual chats, it will not apply to existing chats, nor will it automatically apply to groups you are in (you can however separately set those groups to have disappearing messages)
- Once all messages have disappeared from a chat, the chat will still appear, which may look very suspicious
- A preview of the message can persist after it has disappeared, if it hasn't been read
- If the recipient includes the message in a reply, the included message will not disappear
- If the recipient forwards the message, the forwarded message will not disappear

- If WhatsApp is set to save photos and videos to your Camera Roll/Gallery (this is the default setting; it can be turned off for both iPhone and Android) it will do this even if messages are set to disappear

A victim of abuse may also be on the receiving end of disappearing messages in WhatsApp or another messaging app. If they want to keep the message as evidence they may be able to take a screenshot, but they should be aware of how the messaging app handles screenshots - for example, Facebook Messenger will notify the sender if the recipient screenshots a disappearing message. WhatsApp meanwhile blocks screenshots of 'view once' (photos and videos) material. The safest and most reliable way to record messages as evidence is to take a photo with another device. See Safeguarding Devices for notes on how to save photos etc for evidence.

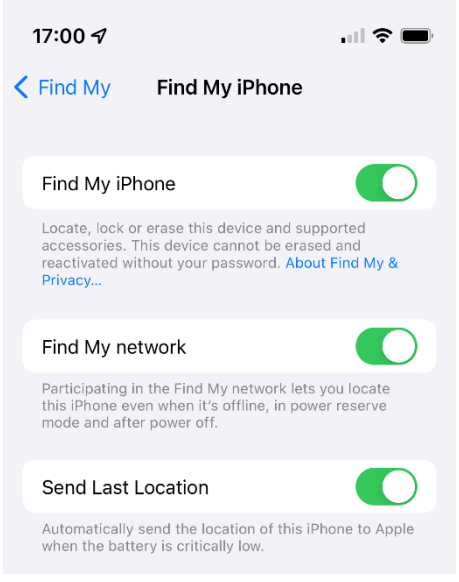
Cloud backups

Devices will carry out backups automatically (if set up). If you share an account with someone else, you will both be able to see anything which is backed up - this can include photos, videos, emails, etc. This can give an abuser access to things you would rather they not see.

Ideally you would have a separate account, with a strong separate password and 2SV/2FA applied. If this is not possible you could:

- Change backup settings to back up locally, e.g. to an external hard drive; this gives you control over what is backed up, and the drive can be kept secure.
- Change backup settings to back up manually, giving you control over what is backed up.
- Select which apps and functions back up, and which do not.

As changes in the way you back up could alert the abuser - e.g. if photos from your phone stop appearing in the cloud backup - you should be cautious in changing backups.



Find My iPhone/Device

iPhone

Apple's Find My network allows users to find their own devices, and devices belonging to friends and family who have given them access. See Air Tags and Bluetooth Trackers for how Find My works with trackers rather than devices. Settings are found under Apple ID > Find My.

To avoid being tracked by an abuser, you could:

- Turn off Share My Location
- Under Find My iPhone:
    - Turn off Find My iPhone - note you will also need to turn off Share My Location for this to work
    - Turn off Find My network - this will prevent the phone being findable if it's offline, in power reserve mode, or turned off (iPhones from 11 upwards can otherwise be found when in these states)
- In the Find My app, remove the abuser (at the bottom of their entry in the People tab)

Changing any of these settings may alert the abuser.

Note: Apple's new Safety Check feature available from iOS16 allows you to immediately stop all sharing and access, and review your security. There is also the option to manage sharing and access, which will show your sharing settings, and allow you to review them along with wider security.

Android

Android includes built-in functions to find devices including phones, tablet, and OS watches. These are designed to find your own devices when signed into your Google account. When location is turned off the function will not find the device, but will allow administration of the device, meaning an abuser with access to your Google account could remotely lock or erase your device.

Devices from different manufacturers will offer different options. These include but are not limited to:

- Turn off Location
- Under settings Find My Mobile
    - Turn off Find My Mobile
    - Turn off Send last location
    - Turn off Offline finding

Changing any of these settings may alert the abuser.

Account sharing

If you are sharing an account, you can hide yourself by reversing the settings in the Find, lock or erase an Android device guidance:

- Turn visibility on Google Play off
- Have Location turned off
- Have Find My Device turned off

Third party apps

Various apps are available to carry out Find-My-like functions. If you have shared your location using one of these you may want to uninstall it or switch it off, or adjust the settings. What you choose to do will depend on how concerned you are that your abuser may be using it.

All URLs

Change notification settings:

On iPhone: https://support.apple.com/en-gb/guide/iphone/iph62faab6a4/ios

On Android: https://support.google.com/android/answer/9079661?hl=en-GB#zippy=%2Cturn-notifications-on-or-off-for-certain-apps

Turn off sensitive content in notifications – Android:
https://support.google.com/android/answer/9079661#zippy=%2Coption-hide-sensitive-content-from-notifications-on-your-lock-screen

Configure WhatsApp media saving settings:

iPhone: https://faq.whatsapp.com/605266123408407/?locale=en_US Android: https://faq.whatsapp.com/365890951034147/?locale=en_US

Apple's new Safety Check feature: https://support.apple.com/en-by/guide/personal-safety/ips16ea6f2fe/1.0/web/1.0

Android – find your own devices when signed into your Google account:
https://support.google.com/accounts/answer/6160491?hl=en

Find, lock or erase an Android device guidance:
https://support.google.com/accounts/answer/6160491?hl=en