Safeguarding Devices

Protecting phones and other devices

All phones and other devices should be locked when not in use. Even if someone is not at risk from a specific abuser this will prevent casual use of a device by anyone who happens to be able to pick it up. Lock settings on different devices include:

- The method used to unlock the device - e.g. PIN, password, fingerprint, face recognition.
- Automatic locking after a specified period of time

While convenient, fingerprint and face recognition can be a problem in a domestic abuse situation. An abuser can use the victim's fingerprint to unlock the device while the victim is asleep or unconscious. Face recognition can usually be set to allow recognition of a face only if the eyes are open. This feature is called Require Attention for Face ID on iPhone, and variations on Require Open Eyes on Android. If a victim wants to use face recognition, these options should be switched **on** to ensure they need to be awake to unlock the device. It would be wise to test how well this works in practice. If face recognition is available, but the requirement for eyes to be open is not, it would be best not to use face recognition to unlock the device.

Note: Testing by Which? has shown that face recognition on some phones is unreliable, and can be bypassed using a photo of the owner. This affects mostly cheaper phones that may be used as 'burners', but does include some more expensive handsets. If in any doubt about the security of face recognition, use a PIN or password instead.

Many apps will be accessible without further verification once the device is unlocked, for example social media and email. This means having the most secure lock possible on the device itself is important, but still means an abuser can have access to sensitive information if they can just unlock the phone.

Some apps can be set to use biometric ID, i.e. fingerprint or face recognition, to unlock. This includes banking apps, and other apps which would otherwise use different credentials to the main device (i.e. you cannot access a banking app with just the phone PIN). Even if a victim has chosen to use biometric ID for their device, they should not use it for apps on the device. PINS or passwords should be used for any apps that support them.

Note: This article mostly protects against abusers with physical access to a device. See App protection and sharing for information on preventing remote access to data and location information. In particular Apple's Safety Check

feature available from iOS16 allows you to immediately stop all sharing and access, and review your security; or to carry out a review of sharing, access, and security.

Saving private files on a device

A victim of abuse may want to keep certain files private from their abuser, including because they are trying to build up evidence against the abuser. There are two considerations for the victim when saving private files:

- Can the abuser tell they have hidden/locked a file?
- Can the abuser access the file?

These methods, and others that are available, are highly variable regarding the first question. They are less variable with the second - files can be locked with similar methods to the phone itself. However no method is entirely private or secure if the abuser has access to the device, and is determined.

An alternative method to saving private files on the victim's own device would be to send them on to a person who they trust, whose device is highly unlikely to fall into the hands of the abuser. If they do this, they should take care to remove all evidence (the original file, and messages containing it) from their own device.

Samsung (Knox) secure folders

Secure folders are included as standard on newer Samsung phones, using the Samsung Knox framework. You can set up and use a secure folder using different protection to the main device - a different PIN, password or pattern, or (on some phones) a different fingerprint to the main one.

The secure folder can contain many different types of content, so a victim could use it to store photos, videos, files, emails, notes, etc, for example: photos of injuries, screenshots of attempts to access data, diarised events, and so on.

A secure folder, set to be hidden, may be a useful way to store files that a victim does not want their abuser to see. However there are ways that an abuser could discover that a secure folder is in use, especially if they know what they are looking for and/or have extensive access to the device. These include:

- When you go into secure folder settings, the device will ask for a PIN/biometric
- On rebooting the phone a notification will appear if a secure folder is in use
- If a user turns off the screen while in the secure folder, or using an app in it, when the phone is woken it will immediately ask to unlock the secure folder

If the secure folder is not hidden, then certain apps, e.g. Gallery, will also have an option to move items to the secure folder directly from the regular app, which could alert the abuser to its existence.

Masquerading apps

Apps are available that provide support for victims of abuse while appearing to be something else. For example, Bright Sky appears as a weather app but contains information, guidance, and a secure place to keep evidence of abuse. Numerous covert messaging apps are also available.

While these may have some use for victims of abuse, they should be used with caution while in the relationship, especially if the abuser is likely to access the phone. Even if just glimpsed, it's easy to look up the name of an app and discover it's not what it seems.

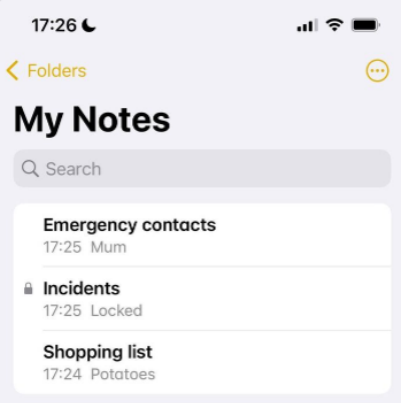
Other secure folders

Third party apps with similar functionality for iPhones and other Android phones and devices can be downloaded through their App stores. A victim wanting to use one of these would need to look carefully at functionality for such an app.

App-specific hiding and locking

There are a number of ways on different devices that specific file types (e.g. photos or notes) can be locked or hidden, for example:

- Hide photos on your iPhone, iPad or Mac
- How to lock or unlock notes on your iPhone or iPad
- Hide your sensitive photos and videos – Google Photos Help
- Protect your files with safe folder – Files by Google Help



Android features may be device-specific.

Some of these features are more secure than others - photos on iOS can be hidden quite thoroughly, while locked notes are clearly visible in the Notes app (and the title, if there is one, will be visible. If someone has extensive access to a device, and is determined, it is unlikely they will miss that secure folders, or hidden or locked content, are in use.

Using a SIM PIN

A SIM card is a removable card that stores your phone number. If someone removes the SIM from your phone, and inserts it into a their phone, they will be able to:

- make calls and send messages that appear to be from you
- receive calls and messages intended for you

If someone has put your SIM in their phone, and you've used your phone number to secure an account using 2-step verification, then they will receive the code via text message.

However if you set up a 'SIM PIN', then you must enter a PIN when:

- a SIM is put in a new device
- a SIM is returned to the original device
- any device containing the SIM restarts

Note: Most people do not set a PIN for their SIM; it protects against very specific 'attacks' and comes with some risks. It may be a useful measure for a victim of domestic abuse who is specifically concerned about their abuser using their SIM in another device.

Important to know: although SIM PIN is not *activated* by default on phones, there is a PIN set for your SIM (usually a default number depending on your mobile provider). You will need to enter the default PIN before setting your own PIN. You have three attempts to get it right, after which your phone will need to be unlocked by the provider, so be careful.

The default PINs for the four major UK mobile providers (EE, O2, Three and Vodafone) can be found online, along with most of those for the virtual providers (eg GiffGaff, Sky Mobile etc).

How to ...

Set a SIM PIN on iPhone:
Settings – Mobile Data – SIM PIN – toggle SIM PIN on

Set a SIM PIN on Android (example – specific phones may vary):
Settings – Security – Advanced – SIM card lock – toggle Lock SIM card on

What should I set my SIM PIN to?

SIM PINs can be between 4 and 8 digits long. Like any PIN, they should not be easy to guess, either for anyone (so not 0000 or 1234) or for someone who knows you (so not your date of birth).

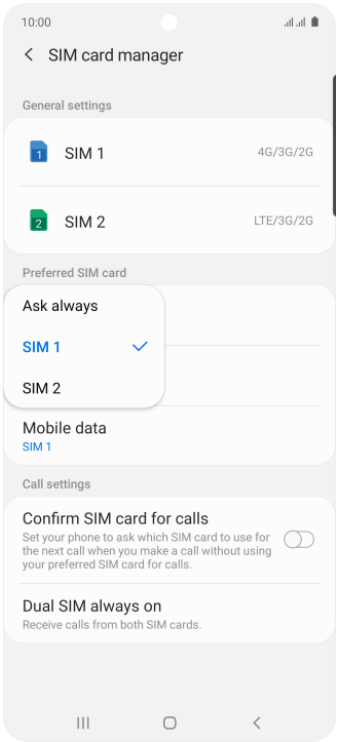
Note: It's okay to have the same PIN for the phone and the SIM. If someone 'needs' to put the SIM into another device, it's because they don't know the phone PIN.

Be aware:

- It's not common to use a SIM PIN, so setting one may tip off your abuser that you are actively trying to deny them access.
- If the abuser tries repeatedly to unlock the SIM in another phone, the SIM will be locked after three attempts and be unusable in the any phone.
- Using a SIM PIN will tip you off that someone has removed your SIM from your device and then replaced it, as you will need to input the PIN when you next use your device.

Note: switching a physical SIM from one device to another like this does not constitute a 'SIM swap' attack, which is a more 'sophisticated' remote way of taking over a phone.

Dual SIMs



Several phone models have a dual SIM feature, meaning that they can operate two phone numbers using only one handset. The additional SIM can be a physical item like the main SIM, or for some devices it can be an eSIM, which is not a physical object.

A dual SIM does **not** offer protection for a victim who is still in the relationship. Most content, including recent calls and any texts made or received, will be visible on the phone even when the second SIM Is not installed.

For a victim who is still in the relationship, the most straightforward way to keep communications and content away from their abuser would be to acquire a second, 'burner' phone and keep it away from the abuser.

A second SIM could be of use for a victim who has left the relationship but still needs to keep up some degree of contact with the abuser. This would allow them to control when the abuser can contact them by removing or deactivating the SIM when

they don't want to be contacted. It could also allow them to start to build a new life with a new phone number unknown to the abuser.

Emergency alerts

Emergency Alerts is a UK government service that will warn you if there's a danger to life nearby. In an emergency, your mobile phone or tablet will receive an alert with advice about how to stay safe.

This function could let an abusive partner know about a secret or secondary phone. It is possible to opt out on both iPhone and Android.

iPhone: To opt out, search your settings for 'emergency alerts' and turn off Severe alerts and Emergency alerts. If this does not work, contact your device manufacturer. For further advice go to gov.uk/alerts/opt-out

Android: To opt out, search your settings for 'emergency alerts' and turn off Severe alerts and Emergency alerts. On Huawei devices running EMUI 11 or older, search your settings for 'emergency alerts' and please turn off "Extreme threats", "Severe threats" and "Show amber alerts". If this does not work, contact your device manufacturer.

Refuge have produced a guidance video.

All URLs

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

Samsung Knox:

Set up and use a secure folder: https://www.samsung.com/uk/support/mobile-devices/what-is-the-secure-folder-and-how-do-i-use-it/

Set it to be hidden: https://docs.samsungknox.com/secure-folder/Content/show-hide.htm

Hide photos on your iPhone, iPad or Mac: https://support.apple.com/en-gb/HT205891

How to lock or unlock notes on your iPhone or iPad:
https://support.apple.com/en-gb/HT205794

Hide your sensitive photos and videos – Google Photos Help:
https://support.google.com/photos/answer/10694388?hl=en-GB

Protect your files with safe folder – Files by Google Help:
https://support.google.com/files/answer/9935264?hl=en-GB

Emergency alerts:
https://www.gov.uk/alerts

Refuge guidance video to turn off emergency alerts:
https://www.youtube.com/watch?v=I2MBcHwmiy8