LOCATION SHARING

Location sharing lets other people know where you and your device are without having to call or text them.

This can be useful when meeting up with friends, keeping track of family members or help you find lost items. **But** like lots of useful tools, it can be dangerous in the wrong hands. No one wants to be followed home, or have their ex turn up unexpectedly on a night out.

So here are some things to consider before sharing your location freely with everyone in your phone...

Know which apps use location sharing

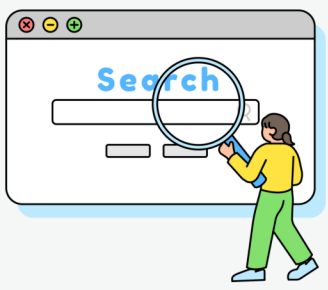
Some apps need location sharing to work - Google Maps won't be much use if you don't enable it – but with most apps, you should have the option to only 'share whilst using the app'.
Not only does this protect your privacy, it also saves your battery life as GPS tracking, which makes location sharing work, normally uses a LOT of battery.

Know who you're sharing your location with

Is it being broadcast to all users of the app, or just your 'friends'? Do you really want total strangers knowing where you are at any time, day or night?

Check the app's security record before enabling location sharing

Some apps not only share your location with other users of that app, but also pass that data on to other companies for marketing purposes. The more people who have your data, the more chance of a breach – so check privacy policies before you use any new app. You can do this easily with a quick internet search using the name of the app and terms like 'privacy' or 'data breaches'. **If you don't like what comes up, avoid using it.**



Think before you 'check in'

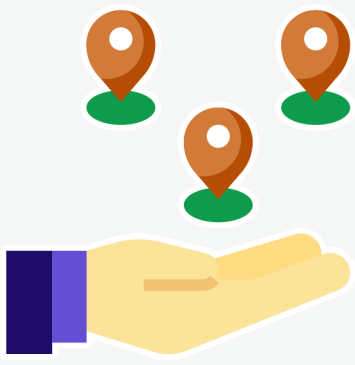
'Checking in' at a venue can be a fun way to let friends know where you are and what you are doing – but bear in mind that it also lets people know when you are away from home. If you use it regularly, criminals could potentially build up a picture of your daily routine and use that to target you or your home.

How to control location sharing

There are two main ways to control location sharing in your phone

1. **going to your phone settings and switching off location sharing.**
2. **going into individual app settings and setting permissions.**

If you aren't sure how to do this, there are lots of guides online – type in the name of your device and 'location sharing settings'.



Do a regular check

With all the different apps you use, it's can be easy to lose track of what permissions you have given – so it is a good idea to regularly check through your apps list and turn off location features for any you aren't currently using.

TWO STEP VERIFICATION & BIOMETRICS

Two step verification (2SV) or **two factor authentication (2FA)** are ways to add extra protection to accounts. Both mean that something extra is needed, in addition to username and password, to get into an account.

This is usually an SMS sent to your phone (which means only the person holding the phone can access the account) but there can be other methods.

2SV/2FA can:

- **Alert you to attempts made to access the account.**
- **Prevent certain activities happening, e.g. payments being made.**
- **Help to build evidence against an abuser.**

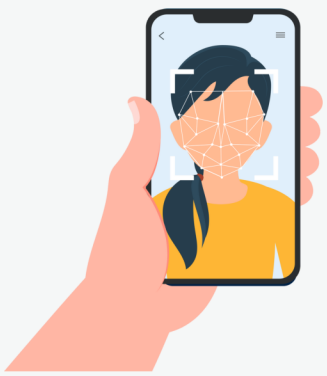
Never share the codes sent as part of 2FA/2SV with anyone as this will allow abusers access into your accounts.

To set up two factor authentication, go to your device Settings and select 'Security' or 'Sign In & Security', then follow the prompts.

Biometrics

Biometrics means using parts of your body to identify yourself. Some devices offer the option to set up biometric security features.

Examples of this includes fingerprint access, facial recognition and voice recognition. These are mostly used instead of, or with, a passcode, to unlock your device.



Finger print and face recognition

While convenient, fingerprint and face recognition can be a problem in a domestic abuse situation. An abuser could use the victim's fingerprint to unlock the device while the victim is asleep or unconscious.

For this reason, if fingerprint ID is used to unlock the device, it is not recommended that it also be used to access apps such as email and banking – passwords offer greater security.

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 **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.

BLOCKING ACCOUNTS AND REPORTING ABUSE

If you are experiencing abuse online, it can be hard to know what to do for the best.

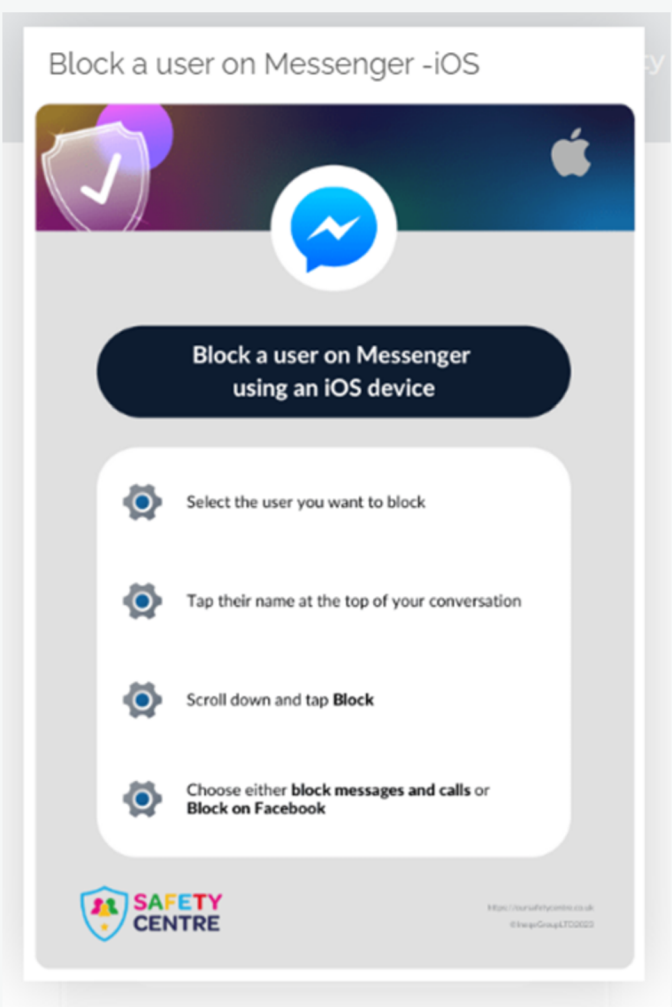
However, **there is lots of support available online**, and many steps you can take to protect yourself without involving the police.

If you believe a crime may have been committed, and you decide that you want to report to the police, talk to your support worker about the best way for you to do this.

How to report harmful content & block accounts

To report harmful content or block accounts, we recommend using [Home Page - The Online Safety Centre (oursafetycentre.co.uk)]

With this website you can search for the platform you need help with, and view visual guides or videos which will explain the steps you need to take. There are guides for Apple Phones, Android Phones, and Desktop devices.



Another useful website is [Report Harmful Content - We Help You Remove Content].

If you have already asked a platform to take down harmful content, and they have not responded within **48 hours,** this site can help you get harmful content removed e,g, revenge porn. It also provides useful guides about when to report to the police.

It can help with the following types of harmful content:

- Threats
- Impersonation
- Bullying & Harassment
- Self-harm or Suicide
- Online Abuse
- Violent Content
- Unwanted Sexual Advances
- Pornographic Content

1625 Independent People

CHOOSING AND USING PASSWORDS

Top tips

- Choose strong passwords
- Change passwords regularly
- Don't use the same passwords for multiple accounts
- Don't share accounts

Choosing strong passwords

DO

- Use a minimum of 12 characters
- Use special characters, letters & numbers
- Use upper and lower case
- Keep it random

Choosing strong passwords

DON'T

- Use names, birthdays or house numbers
- Use easily recognised sequences
- Use common words or phrases

3 ways to create a strong password

1. **Use three random words** and change some of the letters into numbers or special characters – for example E could become 3 or i could become !

2. **Use a shortened sentence**
e.g. My favourite aunt's name is Susan and she makes great trifle
Becomes: MfaniSasmgt
Add some numbers or special characters to make it even stronger.

3. **Use Auto Generation**
Use an online Random Password Generator, or allow your device to auto generate a strong password for you. These passwords are hard to remember, which is why they are strong – so use a password manager to store them.

In domestic abuse situations it is best not to write passwords down, because of the risk that the abuser might find them.

You should change your password:

- Any time you have shared your device or account with someone else
- After a break up
- Any time you see suspicious activity on your account
- Any time you forget it, or get locked out of your account

Avoid re-using passwords, or just changing one or two letters or numbers. Changes like these are easy to guess, especially for someone who knows you well.

Think twice before sharing accounts. You may trust someone now, but how easy will it be to stop sharing in future? If you choose to share as a one time thing, make sure you change your password afterwards.

Priority accounts

Some accounts are more important than others. You should always make sure that your email account and your bank accounts have strong, unique passwords. This is because if someone successfully hacks into your email, they can reset all your other accounts. And if someone hacks into your bank, they can take your money.