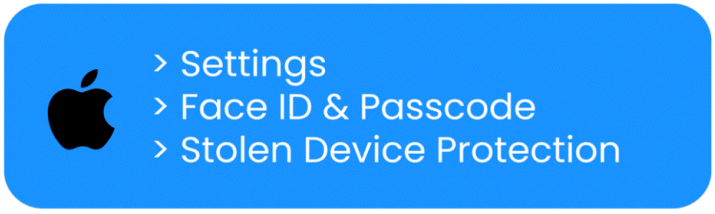
Be Switched On - Extra phone security with a single swipe.

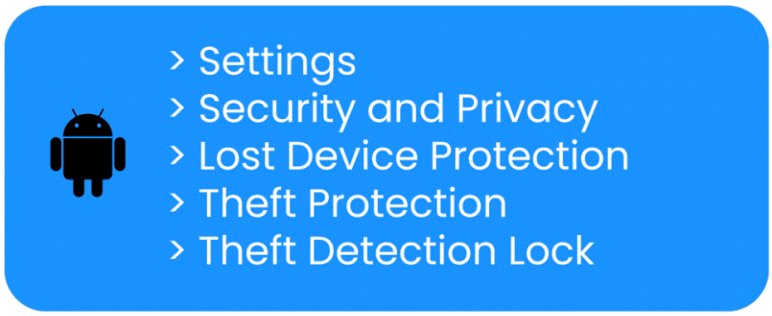
Phone thieves don't just want your phone; they want access to your bank accounts, documents and identity. But by taking a few simple actions, you can slow down the thieves and add an extra level of security to your device, all in under 30 seconds.

Activate anti-theft protection

Whichever phone you use, it is quick and easy to activate your phone's in-built anti-theft protection. For iPhone users, Stolen Device Protection provides an additional level of security when someone tries to access sensitive features or settings from an unfamiliar location by requiring Face ID.

Android users should enable Theft Detection Lock which uses sensors to detect motion patterns that suggest theft (like sudden snatching) and can lock your device immediately.





Take further security steps

There are some other simple steps that you can take that make it much harder for criminals to access the contents of your phone if it is stolen. Taking these steps now could save you a lot of time, money and hassle in the long run!

1. Keep your software updated

Install manufacturer and app updates as soon as possible to ensure that your phone always has the best protection and security. Ideally set your phone to update automatically in your settings menu.

2. Control your access settings

- Lock your phone when you're not using it and set the auto-lock to activate itself after a short period of time.
- Make it harder for thieves to 'shoulder-surf' your login information by using biometric authentication and strong passwords instead of 4-digit passcodes.

3. Protect your personal information

- Think about whether apps containing sensitive personal information (e.g. banking apps) need to be on your phone at all - some may be better kept on a tablet or other device that you don't routinely carry with you. Also try to avoid storing photos of personal information including your ID documents (passport, driving license) on your phone – these can be used by criminals to apply for loans or get round security protocols.
- Secure any apps which contain your personal or financial information (such as email, payment or banking apps) with strong, separate passwords which are different to your phone's access passcode.

- On iPhone, activate biometric protection or hide apps that contain sensitive financial information – access this with a long press on the app's icon. You can also protect photos of sensitive information by pressing them and select 'hide'.
- On Android, protect apps and files (including photos of ID) by moving them to your Secure Folder.
- Don't store PIN numbers, passwords or information about financial accounts in a 'notes' app. Lock notes which contain other personal information by pressing and holding on the note.
- For advice on how to create strong passwords, and further guidance on what you should do if you fall victim to fraud or cybercrime you can find more information in The Little Guide series.

4. Be aware of your surroundings

Be mindful of who's around you when you're using your phone in public, particularly when entering your PIN number or passcodes. Avoid entering personal information in a public space wherever possible.

Never give your phone to people you don't know, particularly if you have just met them. Thieves may ask to borrow your phone or offer to enter their number – don't let them.

5. Turn off message previews

Turning off message previews can prevent thieves from seeing messages on your screen from your bank, or other secured platforms, about reset or login codes when your phone is locked.

6. Get your IMEI number

Your phone's IMEI can help you track it down if it's lost or stolen. You can get your IMEI number by typing *#06# on your phone keypad. Keep a note of it somewhere other than your phone. Your network operator can use the IMEI number to block your device if it is reported stolen.

Has your phone been stolen?

Report it to police as soon as you can. If you've been hurt, feel unsafe or the crime has only just happened, call 999 now. You can still report it afterwards on 101 or online. Then do the following as soon as you can:

- Block your phone via another device as soon as possible - using 'Remote Lock' on Android or 'Lost Mode' on iPhone. You can activate 'Remote lock' on Android by opening your Settings app, then search for and select 'Remote Lock'. Turn on the feature, verify your phone number, and set up a PIN or password as prompted. You can then use the android.com/lock website to lock your phone from another device by entering your phone number and answering the security questions. To activate 'Lost Mode' on an iPhone, open the 'Find My' app on another Apple device or go to iCloud.com/find on a web browser.
- Notify any financial app providers associated with your phone - Freeze your cards or accounts to help prevent fraudulent transactions being made or loans being taken out. Any transactions made after your phone has been reported stolen may be reimbursed by your bank.
- Notify your phone provider - This will ensure that two-step verification (2SV) messages do not get sent to your number.
- Change your passwords - Changing your passwords means that criminals will no longer be able to access applications on your device. You should prioritise securing your email, social media and banking applications first.
- Keep an eye out for unusual activity - If you spot any unexpected behaviour after a theft, for example, transactions on your accounts or email notifications of an account sign-in, change the password for that account.