

## LOSING YOUR SMARTPHONE OR HAVING IT STOLEN CAN BE A MAJOR TRAUMA.

There are things that you need to do in order to make things less stressful and expensive. The specific details on different models and operating systems vary. This guide will, hopefully, help you to limit the consequences and help to recover from the loss or theft.

### HAVE A SPARE SMARTPHONE

It is a good idea to have a second phone. Keep your old phone. It does not need a SIM as it can still access the internet over your home wifi. (Keep it up to date as far as possible, just like your normal phone). You can still make calls through WhatsApp, Facetime, etc, and access your email and the internet. This is especially important if you don't have a laptop or PC.

### KNOW YOUR PASSWORDS

It is important to have all your login details saved somewhere else **away from your phone**. Your Gmail accounts are always accessible over the internet.

For Apple it is vital to have your **Apple ID** in order to access your account including Find my Phone.

For Android you need your **Google account** login and, perhaps, another login for your phone's brand (e.g. Samsung).

Also, make sure you know login details for your Microsoft and Google accounts and any other email accounts that you have including your mobile phone service provider. Most logins can be recovered using your email address and the "Lost Password" option.

### YOUR LOGIN DELAY

If Face ID is not available, the phone will need a login code to re-open it. It is tempting to make the auto-login time longer for convenience. **Not a good idea!** A thief who has grabbed your phone will quickly try to use your open phone. (**Apple:** Settings/Display & Brightness/ Auto-Lock. **Android:** Settings/Display/Screen Timeout/ Auto Screen off.) **NEVER SET THE AUTO-LOCK TO "NEVER" as anyone that steals or finds your phone will be able access everything on it!**

### BACK UP EVERYTHING AUTOMATICALLY

Make sure everything on your phone is saved, usually in the cloud using iCloud, Onedrive etc. This enables you to restore things easily to a new phone. Don't save documents, files and photos only on a mobile device. Use, for example, Onedrive, iCloud, Dropbox or Box. Make sure photos are automatically uploaded using **Camera Roll** or similar on your phone.

Email (such as Microsoft/Outlook, Google/Gmail, etc.) is usually kept in the cloud. Your device just has a copy of messages on your phone.

Apps like WhatsApp, Signal, etc have backup features.

### TWO-FACTOR AUTHENTICATION

Many web sites, especially banks, require two-factor authentication these days. If your phone App has biometric security such as Face Recognition, this should be no problem. If the site needs to send a text to your mobile phone, this means you can't login to your bank. (It might even allow a thief to get into your bank). If a site sends you an email, this is ok as long as you can get your email on another device.

All your primary accounts, such as Apple, Microsoft, Google, etc, should be protected with two-factor authentication on multiple devices.

Authentication apps (e.g., Microsoft and Google) can be set up on several devices, such as your main smartphone, spare smartphone, iPad and your PC.

## QUICKLY FIND AND DISABLE YOUR SMARTPHONE

You have to act quickly to locate, lock down or erase your device. So, make sure you know how to do this. If you have both an iPhone and an iPad, you can mark as lost or erase your iPhone/iPad through the "Find My" App on either device.

Apple and Android can locate and lock down your device. [iCloud](#) and [android.com/find](#)

## SAVE YOUR DEVICE DETAILS

Keep a record of your device's details away from your phone. This is important for reporting the theft, claiming insurance etc.

**MAKE:** Apple, Samsung etc.

**MODEL:** The exact model, e.g. Apple iPhone 13 Pro Max.

**MODEL NUMBER:** The model number of your specific device.

**SERIAL NUMBER:** The manufacturers ID of your device.

**IMEI:** All mobile phones have a unique IMEI number.

These numbers are shown within your phone's settings or on the original packing.

Your IMEI can be obtained by dialling \*#06# on your phone.

Always tell the police. The police can add the IMEI to a data bank to prevent it accessing any mobile network. (In theory.)

## BLOCKING AND REPLACING THE SIM CARD

A thief can take out your SIM card and put it in another phone, allowing a thief to use your data. You must login to your provider's web site and block the SIM and request a replacement SIM. The replacement should arrive promptly. If, as mentioned above, you have an old phone you can use the internet through your home wifi until you get a new phone.

## AFTER THEFT SCAMS

Thieves might try to scam you after your phone is lost or stolen. Criminals might pretend to have found your phone and launch a phishing scam to get your login details. Be very suspicious and don't click on any links.

## FINALLY

If you prepare in advance for the loss or theft, it will be much less stressful and difficult if the worst should happen.

18/03/23