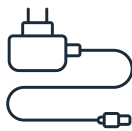




## PROTECT YOUR MOBILE DEVICE



Set an automatic lock on your device with a PIN, password or biometrics such as face ID or fingerprint



Don't use chargers supplied by third parties or public charging stations (such as those available at airports or hotels)



Never leave your device unattended



Ensure software is updated regularly



Only download and install apps from trusted sources such as the official app stores



When you finish, log out of websites and applications, especially banking or government websites

# PROTECT YOUR MOBILE DEVICE

## STEP BY STEP MOBILE DEVICE PASSWORDS

Configure password, PIN, or biometrics such as FaceID or fingerprint to unlock, install any new applications or make any changes to your portable device.

A mobile device with no password protection is an easy target for cybercriminals.

### Apple iOS

1. Go to Settings, then do one of the following:
  - On an iPhone with Face ID: Tap Face ID & Passcode
  - On an iPhone with a Home button: Tap Touch ID & Passcode
2. Tap Turn Passcode ON or Change Passcode.

To view options for creating a password, tap Passcode Options.

The most secure options are Custom Alphanumeric Code and Custom Numeric Code.

### Samsung/Android

1. Go to Settings
2. Tap Security or Lock Screen
3. To pick a kind of screen lock, tap Screen Lock Type or Screen Lock
4. If you've already set a lock, you'll need to enter your PIN, pattern, or password before you can pick a different lock
5. Tap the option you'd like to use. Follow the on-screen instructions.

### Windows devices

1. Go to Start
2. Tap or Click Settings
3. Select Accounts
4. Select Sign-in Options
5. Tap or Click Select Password
6. Select Change.

## STEP BY STEP

# LOCK YOUR MOBILE DEVICE



Configure your device to lock automatically after a period of time to reduce the likelihood of theft.

### Apple iOS

1. Go to Settings
2. Tap Display & Brightness
3. Select Auto-Lock, then set a length of time.

### Samsung/Android

1. Go to Settings
2. Tap Lock Screen
3. Tap Secure Lock Settings and enter your current lock screen credentials
4. Tap Auto-lock when the screen turns off and set a time limit.

### Windows devices

1. Tap or Click the Start menu, then Control Panel
2. Tap or Click Personalisation, then Lock Screen
3. Tap or Click Screen Timeout Settings, then select a time limit.

Unlocked devices can give cybercriminals direct access to information stored on your device - SMS and call history, contacts, emails, social media and messaging apps.

## STEP BY STEP

# CREATE A SIM PIN



Like your mobile device, the SIM card also needs to be protected to minimise the damages to your private data in the event of a phone theft incident.

### Apple iOS

1. Go to Settings > Mobile Data > SIM PIN
2. Turn ON your SIM PIN or turn it OFF
3. If asked, enter your SIM PIN. If you do not know your default SIM pin, contact your network provider to find out
4. Tap Done.

### Samsung/Android

1. Go to Settings
2. Tap on Lock Screen and Security
3. Tap on Other security settings
4. Tap on Set up SIM card lock
5. Toggle the Lock SIM card option (move the slider to ON)
6. Enter your current SIM pin and tap OK to enable SIM card lock. If you do not know your current SIM PIN, contact your network provider to find out.



Cybercriminals can maliciously use mobile SIM cards to access your voicemail SMS, receive passcodes, and make calls anonymously.

STEP BY STEP

## DISABLE LOCATION SERVICES



When not in use, turn off location services to limit the tracking of information that can be used by cybercriminals.

### **Apple iOS**

1. Go to Settings
2. Tap Privacy
3. Tap Location Services
4. Toggle Location Services to OFF.

### **Samsung/Android**

1. Go to Settings
2. Tap Location
3. Toggle Location Services to OFF.

## STEP BY STEP

# WI-FI SECURITY AND PERSONAL HOTSPOT



Cellular data is much more secure than public or external wi-fi when out and about. Setting up a personal hotspot on your device means that your cellular data can be used on multiple or other devices securely (e.g. your tablet or laptop). Or alternatively you can use your mobile cellular data and check your email on your phone, without connecting to any external wi-fi.

### Set up a personal hotspot:

#### Apple iOS

1. Go to Settings > Cellular > Personal Hotspot or Settings > Personal Hotspot
2. Tap the slider next to Allow Others to Join
3. Open your other device (laptop or tablet) and request to join
4. Once access is granted, secure wi-fi (flowing from your mobile device) will become available.

#### Samsung/Android

1. Go to Settings > Connections
2. Tap on Mobile Hotspot and Tethering
3. Toggle on or off Mobile Hotspot to enable/disable this setting.

Please refer to your manufacturer's website or instructions manual for other platforms or operating systems.



Never access your emails from public Wi-Fi in cafes, airports, hotels etc, as skilled cybercriminals can intercept these connections and compromise your device and data.

## STEP BY STEP

# LOST OR STOLEN DEVICE



Lost or stolen devices can significantly jeopardise your personal and economic safety. Cybercriminals can use tools and tricks to recover personal information, saved passwords, bank transactions, personal and work emails.

### If your device is lost or stolen:

- Look for your device on a map

#### Apple iOS

1. Sign in to [iCloud.com/find](https://icloud.com/find). Or use the Find My app on another Apple device that you own. If your Apple device doesn't appear in the list of devices, Find My hasn't been turned on. Refer to other recommendations to protect your device.

#### Samsung

1. Sign in to Samsung FindMyMobile
2. A verification code will be sent to the associated email address
3. Once verified your device will show on the map.

- Mark the device as lost (remotely locks your device).

#### Apple iOS

1. Sign in to [iCloud.com/find](https://icloud.com/find). Or use the Find My app on another Apple device that you own
2. Go to the Devices tab or the Items tab
3. Select your missing device or item
4. Scroll down to Mark As Lost or Lost Mode and select Activate or Enable
5. Follow the on-screen steps if you want your contact information to be displayed on your missing device or item, or if you want to enter a custom message asking the finder of your missing device to contact you
6. Select Activate.

# LOST OR STOLEN DEVICE



## Samsung

1. Sign in to Samsung FindMyMobile
2. Select Lock on the right side
3. Select Next
4. Create a PIN for when you find your phone. You can add an emergency contact and a message that will appear on the device's lock screen if you wish
5. Select Lock.

- Report the missing device to law enforcement.
- Contact your network provider to disable your account.
- Remove the missing device from any accounts or device lists.

Refer to the device manufacturer for a step-by-step guides to remotely find, lock, or erase your lost or stolen device.

## Find and record the device IMEI (International Mobile Equipment Identity)

### Apple iOS

1. Go to Settings > General
2. Tap About
3. Scroll to find the IMEI.

### Samsung

1. Go to Settings
2. Tap About Phone
3. Scroll to find the IMEI.

The device IMEI is a 15- or 17-digit number that can be found in the settings under the general information of your device. Record this number to stop the device from being used in case of theft.







HAVE YOU  
EXPERIENCED  
A BREACH?

**CALL**  
**1800 BREACH**  
(1800 273 224)

