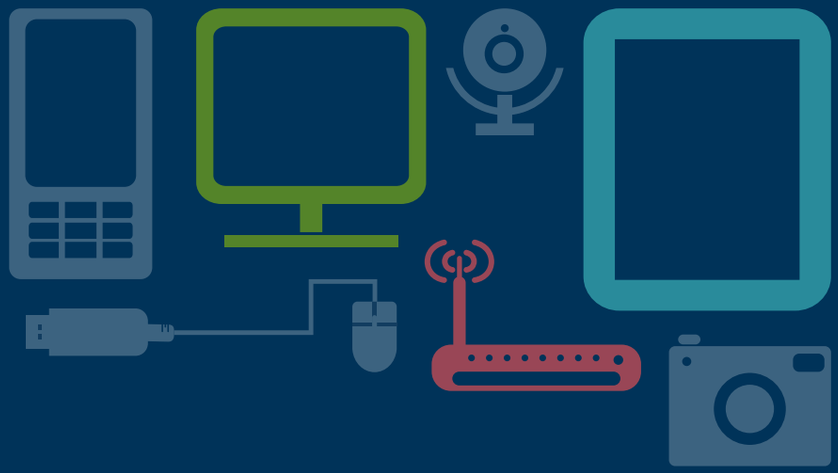
# MOBILE DEVICE SECURITY:

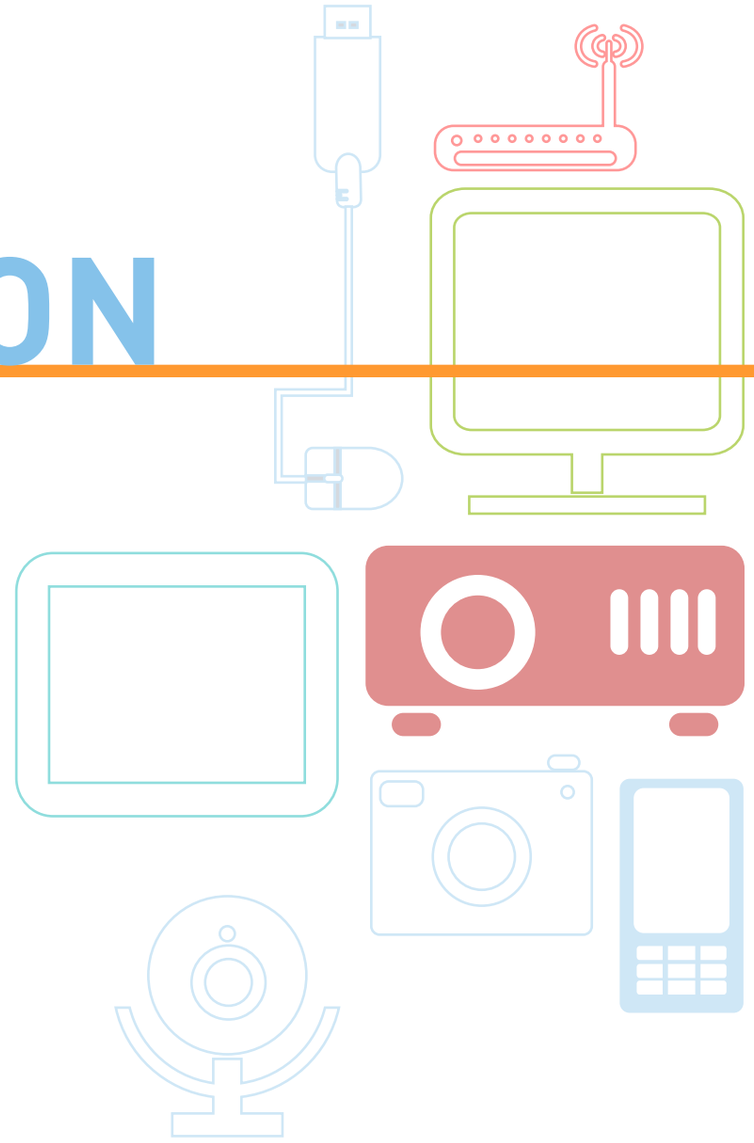
## A buyer's guide to choosing and using mobile devices





Home Office

# INTRODUCTION



**When considering which smartphone, tablet or laptop to buy, there are many things you'll want to consider. But as more of our data is being stored on these mobile devices, it's becoming increasingly important to keep security in mind when choosing (and using) your next device.**

Smartphones, tablets and laptops ('devices') are as powerful as traditional computers, but because they often leave the safety of the house, will need even more protection than your computer at home.

This buyer's guide will help you to compare the security aspects of mobile devices, broken down into 7 key areas. We don't go into detail on how to apply these tips to any one device, but with some online searching and instructions from the manufacturer, they should all be easy to do.

# 1

# CONTROLLING ACCESS TO YOUR DEVICE

**To access your device you'll need to prove you're allowed to use it – typically by using your password, PIN code, or fingerprint. Once you've unlocked it, you'll have access to any online accounts associated with it (e.g. iCloud, Google, Microsoft Live) and securing these accounts is just as important as securing the device itself.**

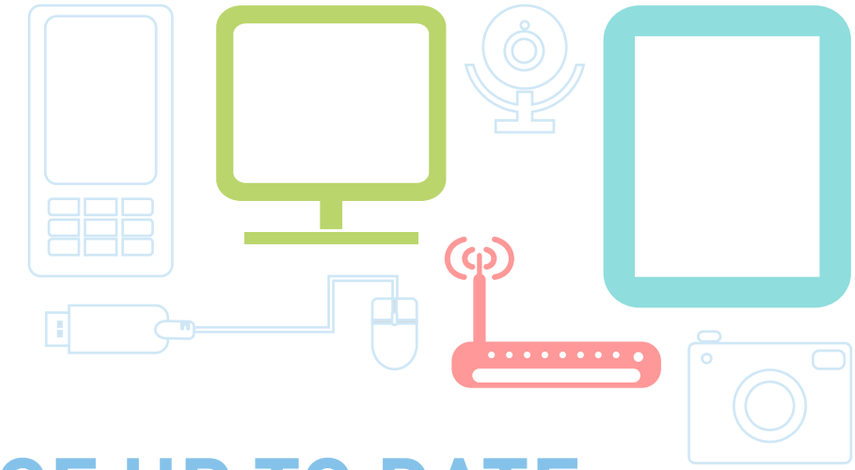
What to look for...

- **Devices that can be unlocked in different ways**. Many devices can now be unlocked using biometrics (such as a fingerprint or face recognition).
- **Online accounts that support 'two-factor authentication' (2FA)**. This is where you'll need to enter a code from an app (or text message) on your phone in order to log into your account. This makes it significantly harder to break into your account if your password is compromised.
- **Devices that reduce your reliance on passwords**. Look for devices that let you make purchases or download apps using a biometric (such as a fingerprint) rather than typing your password each time. This makes it easier to use the device and is often more secure.

Make sure that you...

- **Set a screenlock password, PIN, or other authentication method (such as fingerprint or face unlock)**. CyberStreetwise has some good advice on passwords. If you're mostly using fingerprint or face unlock, you'll be entering a password less often, so consider setting up a long password that's difficult to guess.
- **Secure any linked online accounts**. Strong passwords are one of the best defences against many threats you'll face on the Internet, so set a strong password and turn on two-factor authentication. Don't re-use passwords across devices or accounts. You can use a password manager to help you remember different passwords for all your accounts.
- **Set up security questions that are hard to guess**. Security questions are often used when requesting new passwords from your service provider. Ensure that your answers can't be easily guessed by people that know you, or gleaned from information you've posted on your social media accounts.
- **Follow the manufacturer's guidance**. This will include important information about securing your device and online services.

# 2 KEEPING YOUR DEVICE UP TO DATE



**Keeping your device (and its apps) up to date is one of the best ways to protect it. Manufacturers should make it simple to do this.**

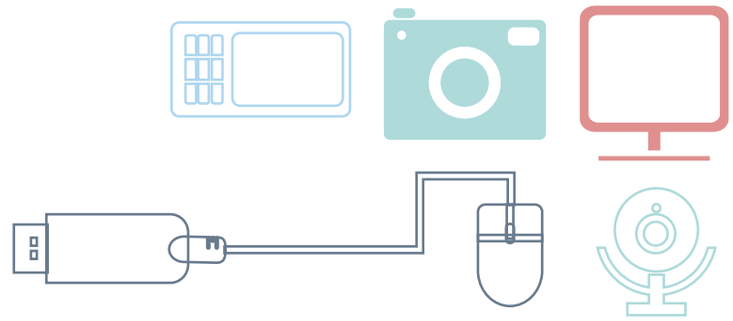
What to look for...

- **How often are devices updated by the manufacturer?** Devices should receive updates several times per year to ensure they are protected from the latest threats. Some manufacturers have publically committed to monthly security updates. The device should automatically check for updates regularly, and let you know when one is available.
- **How long are devices supported by the manufacturer?** Manufacturers will eventually stop providing updates for older devices. Some manufacturers will let you know in advance when this will be. You can use this information to decide when it's time to buy a new device.
- **How often are devices upgraded by your mobile network?** If you're buying your device on contract from a network provider, find out when you can expect your device to be upgraded.
- **How easy is it to update applications?** Apps that you've installed through your devices' built-in 'app store' are easier to keep up to date

Make sure that you...

- **Check that automatic updates are enabled on your device**. Your device will automatically prompt you when updates are available.
- **Apply device updates within a few days of being prompted**. Some devices will automatically update themselves when not in use, but most devices will need you to start the process yourself. You'll often get new features as a result too.
- **Keep your apps up to date**. Check the app store on your device regularly to make sure the latest versions of your apps are installed. If you've installed applications yourself, check regularly to see if new versions are available.

# 3



# USING YOUR DEVICE'S SECURITY AND PRIVACY FEATURES

**Your device's security features can help prevent hackers from stealing your data, or from installing malicious software (known as 'malware'). Devices should be configured to make any attempts to do this much harder.**

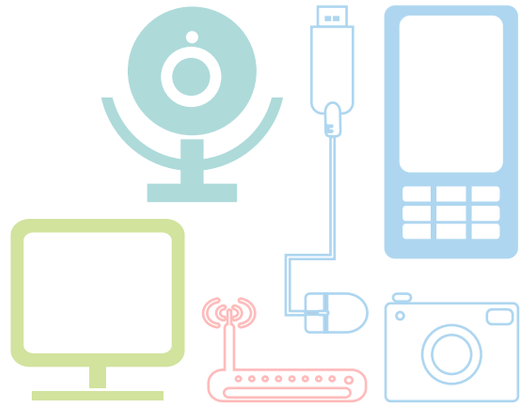
What to look for...

- **Devices running the latest versions of the device software**. In general, newer devices have better security features than older devices, and newer software is better than older software. Look for the latest versions of software and devices, and only consider devices that have those versions.
- **Read the manufacturer's guidance on how to use the security features of your device**. Some manufacturers produce security guides. Read these and get to know what security features your device has.

Make sure that you...

- **Keep your device up to date**. This means you can take advantage of the latest device security technologies.
- **Can trust any external device you're connecting the device to**. When connected to another device (e.g. with a USB cable), the device should prompt you to trust it before syncing data. Similarly, if your device has Bluetooth, be careful what devices you pair with. For example, don't accidentally synchronise all your contacts to a hire car over Bluetooth.
- **Don't disable any of the security features that come with your device**. Even if apps ask you to do this. Similarly, don't enable developer mode, debug mode, or 'jailbreak' or 'root' your device as these will often disable security features as part of the process.

# 4 DETECTING AND PREVENTING MALWARE



**The apps and games installed on your device could be malicious, and can be used by hackers to try and steal your data, or harm your device. GetSafeOnline has some useful information about why protecting against malware is important. You should take steps to prevent malware getting onto your device.**

What to look for...

- **Devices featuring a built-in app store**. These stores only contain apps that the manufacturer has assessed as being safe to install and use. Any harmful apps that are found are removed from the app store.
- **Devices featuring a built-in anti-malware app**. For devices where you can install apps without using the app store, it's important to make sure that malicious apps can't be installed. Anti-malware apps can help prevent this.
- **Devices that let you prevent apps from accessing your data**. Some devices let you know in advance what data (e.g. your calendar or photos) the apps will access once installed. Some devices will also let you prevent apps from accessing that data.

Make sure that you...

- **Only get apps from the device's app store**. Don't weaken any of the security settings on your device, for example by allowing apps from unknown sources to be installed. If you do decide to get apps from outside the app store, then make sure you have antivirus or anti-malware installed to stop malicious apps getting onto your device.
- **Review the permissions that apps ask for**. Only allow the app access to your data if it makes sense. For example, there's no reason why a 'torch' app should ask for permission to access your photos or contacts.

# 5 ENSURING YOUR DATA CANNOT BE ACCESSED

**Encryption turns data into coded information that can only be read if you have the right keys or passwords. Your device should use encryption so if it's lost or stolen (or if you sell it), the data on it cannot be accessed. If the device has removable storage (like a memory card) then that should be encrypted too.**

**You can use internet search engines and manufacturers' guidance to find out if their devices have these encryption features, and how to turn them on.**

What to look for...

- **Devices that have encryption enabled by default**. This ensures your data is protected as soon as you start using the device. Devices should support encryption of sensitive personal data, including messages, email, calendar appointments, photographs and videos.
- **Devices that encrypt the memory card** (if they have one).
- **Devices that support specialised hardware encryption**. This makes it much harder to steal the encryption keys and harder for attackers to steal data.

Make sure that you...

- **Turn on storage encryption if it is not already enabled by default**.
- **Turn on encryption of the device's memory card** (if it has one).
- **Securely erase the data on your device before you sell it**. Use the "Factory reset" feature to quickly delete all your data. Also wipe or remove the memory card before you sell it too.

# 6 USING THE INTERNET SECURELY

**There are many technologies which protect your data when you connect to the Internet, or when the apps installed on your phone connect to online services. You should check that your device has those technologies built-in.**

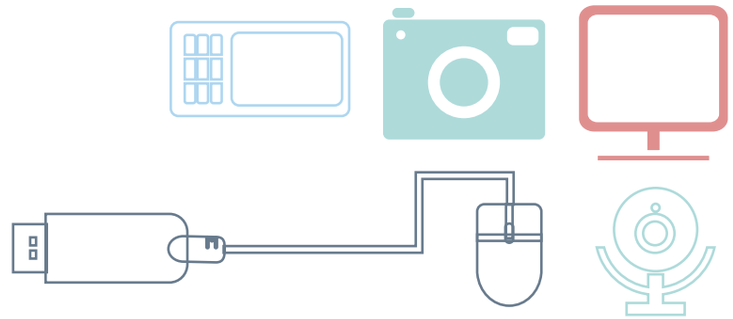
What to look for...

- **Devices with an up to date browser**. Make sure the web browser on your device is up to date. If not, install a reputable browser from the built-in app store.
- **Apps that make public statements about their network security**. Each app is responsible for protecting its own data as it traverses the Internet. Choose apps that make public statements about encrypting all their data safely. This is often contained in the apps' privacy policies.

Make sure that you...

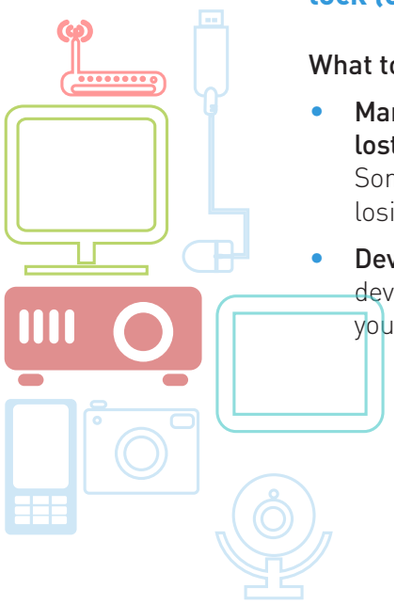
- **Look for the padlock symbol when making transactions on the Internet**. Make sure that you're using the legitimate website of the company you're trying to visit when banking, shopping, or any time you type in passwords or payment details. Make your own way to websites using addresses you've entered yourself, or from search engines.
- **Take care using public Wi-Fi networks**. GetSafeOnline has some advice on protecting yourself when using public Wi-Fi networks. Follow this guidance when you have to connect to a network you don't fully trust.
- **Disable any services and uninstall any apps you don't intend to use**. Apps that come with the device will likely communicate with online services. Disable or uninstall ones that you won't use, as this will prevent any data leaking through these routes.

# 7



# REDUCING THE DAMAGE OF A LOST OR STOLEN DEVICE

**If your device is lost or stolen, then you will want try and locate it, or remotely erase the data. Manufacturers provide websites where you can log in (from a different device), check the location of your lost device, and then lock (or erase) the device remotely.**



What to look for...

- **Manufacturers that include an online service to locate lost devices**. Devices can then be remotely locked or wiped. Sometimes you'll need to enable this feature yourself before losing the device.
- **Devices that can automatically backup your data online**. If your device is lost or stolen, you can still wipe the device but recover your data from the backups.

Make sure that you...

- **Turn on the anti-theft features on your device before you have a chance to lose it**. Ensure you know which website to use (and your login details) so you can locate, lock or wipe your device.
- **Turn on automatic backup if it's available**.
- **Set a PIN on your SIM card**. This can be used to stop a lost or stolen device from being used to make calls which would be charged to you.
- **Read the Home Office advice on** how to reduce mobile phone theft.