SPYWARE & DIGITAL SECURITY

SPYWARE

Spyware is the name given to apps or software that can be downloaded on to your phone, tablet or computer. Once downloaded it can record your activity and feed it back to the person who installed it. It can also be used by that person to access things like your location, photos and texts, and to record calls or even intercept calls or emails before you get them.

Someone usually needs to have physical access to your device in order to download spyware. For example, if someone gifted you a phone and set it up for you, or if someone knows your passcode and might have gone on your phone without you knowing. However, spyware can also be installed by sending someone a link, for example in an email, and then getting them to open the link on their device. Links can sometimes be disguised to make you think they are for something else such as your online banking or for a special offer at a store.

It is very difficult to find spyware as it's designed to be secretive. Your device might behave a little differently if it has spyware on it, so that can be a good clue that it's there.

For example:

- It's unusually slow to respond
- The battery runs out quicker than usual
- It gets hot when you're not using it
- You get unexpected advertising messages or notifications
- You get odd text messages that contain random symbols or numbers
- You see new toolbars, search engines or internet home pages that you don't recognise
- The data usage is a lot higher than you expected
- You hear odd sounds or distant voices on calls
- Shutdown or start-up times are longer than they should be

There are some checks you can do to help you tell if there is spyware on your device:

iPhone / iPad

It is difficult to install spyware on an iPhone as Apple has strong security restrictions. To install it an iPhone has to be 'jailbroken' first, which means the security restrictions are removed.

To tell if your iPhone is jailbroken go to settings. In the search bar at the top of the screen search for apps called Cydia and SBSettings. If either are found then your phone is jailbroken and possibly has spyware on it.

To un-jailbreak your phone you can delete these apps and then restore the phone to normal secure settings by doing a full factory reset. A factory reset will wipe everything on your phone, so make sure you have backed up everything first. Instructions for a factory reset can be found online.

Android Phones / Tablets

There are a few ways you can check for spyware on android devices:

- Look in settings and you'll see a setting which allows apps to be downloaded and installed that aren't in the Google Play Store. If this has been enabled, it's a sign that spyware may have been installed.
- Spyware apps will often have no icons so you won’t be able to see them on your home screen, but they might still show up in the main apps list. Be aware that they might have an innocent sounding name that you wouldn’t relate to spyware. Go to settings > apps and notifications > see all apps and check what’s there. Delete anything you don’t recognise or seems unusual.
- Spyware apps can also be hidden in the settings menu. Look for menu items that don't look right or that you haven't noticed before.
- There are 3 Android apps that will scan your phone and tell you if you have any spyware installed. Try downloading one of them: Incognito, Certo, and Kaspersky Antivirus.

Computers

You can see everything that is running on your computer by doing the following:

- For computers that use Windows: Open Task Manager (search for it in the taskbar search box) to see everything running.
- For computers that use macOS: Open Activity Monitor (search for it in Spotlight via Cmd+Space) to see everything running.

Remember spyware will probably have a name that will stop you getting suspicious, so you need to carefully check through everything that comes up. If you see anything you don't recognise or that just seems odd, then do an internet search for it and that will usually tell you what it is.

A complete system reset for Windows or macOS should clear the majority of spyware. You can search on the internet to find out how to do this. Make sure you back up your files first.

Removing Spyware

If you have a strong reason to believe there is spyware installed on your device you should report it to the police by calling 101. It is a form of stalking and is a crime.

If you do manage to find spyware apps you should think carefully before deleting them as the person who installed the spyware is likely to find out and this might put you at risk.

If you feel you might be at any risk it is often best to continue using the devices whilst being careful what you do and say on them, in order not to alert the person spying on you. You can then obtain a new pre-paid phone that you can use for private conversations, and you can speak to the police or other specialist stalking or abuse organisations who can help you decide what to do next.

KEEPING SOCIAL MEDIA ACCOUNTS SECURE

Look through the activity on your accounts, for example messages that have been received and sent, or friends that have been made or requested to see if there’s anything you don’t recognise as this could be a clue that someone else is accessing your account.

Check to see which devices you're logged into your accounts on by going to the account settings and looking at the security and / or login settings. All of the devices your account is used on will be listed.

Some accounts, like WhatsApp and Snapchat, can only be used on one device at a time, so you know that the login you're using is the only active one. Other accounts like Instagram and Facebook can be logged in to on more than one device at a time, so someone else could be using your account too.

Remove any devices you don't want to be logged in on, and the next time anyone tries to access the account on the removed device they won't be able to automatically log in, they will have to put the password in first. Make sure you change your password if you remove a device so that the person who was accessing your account can't get back in.

KEEPING YOUR EMAILS SECURE

Look at the activity on your email account, like what's in your sent folder, drafts folder and trash. If there are messages you don't recognise or which seem suspicious then someone else might have access to your account.

If someone else has gained access to your emails they might have set up an automatic forwarding function, which means any emails you get might never appear in your inbox and might instead go straight to a different account. How to check for this will depend on your email provider. Do an internet search to find out how.

PROTECTING YOURSELF

- The most important thing you can do to stop anyone accessing your email, social media and other accounts is to choose a secure password (use upper and lower case, numbers, random characters, do not use passwords related to names, places, significant dates etc), keep it private and change it regularly. If anyone does get access to an account they will be kicked out when you change your password.
- Turn off location settings on your phone to stop people and apps being able to track your location. On iphone got to settings > privacy > toggle the location services switch to off. On Android phones go to settings and look for either the connections tab or, depending on your phone, the privacy tab. Tap location and toggle the switch to off. You can also switch off location-tracking features on emergency location service and Google location sharing if you have an Android phone.
- Set a strong passcode on your phone and change it regularly. Turn off the fingerprint and facial recognition login in case someone tries to unlock your phone with these whilst you are asleep.
- Check your security and privacy settings on all apps and accounts. Set everything to the highest security setting and turn off any location tracking permissions. You can do an internet search to find out how to do this for each app you use.
- Keep your software up to date – always instal new updates as soon as you're notified of them as they feature extra security settings.
- Don't give anyone access to your phone – someone usually has to physically have your phone for a period of time in order to install spyware, so keep it on you.

USEFUL RESOURCES

Police – 999 (emergency) / 101 (non-emergency)
National Stalking Helpline - 0808 802 0300
Paladin National Stalking Advocacy Service - 020 3866 4107
National Domestic Abuse Helpline – 0808 2000 247

https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/
https://www.refuge.org.uk/our-work/forms-of-violence-and-abuse/tech-abuse-2/resources/