Online Safety Guidance for Domestic Abuse Victims

Bitesize

WEST YORKSHIRE POLICE

Passwords

It is vital you follow the Government advice of using 'Three random words' as your password. It is acceptable to use the same passwords for all your accounts excluding your email account. Protect your email by using a strong separate password. Consider changing your wireless router password and default router password too for more security.

Two-factor authentication (2FA)

Two-factor authentication (2FA) provides a way of 'double checking' that you really are the person you are claiming to be when you are using online services, such as banking. When setting up 2FA, the service will ask you to provide a 'second factor', which is something that you can access. This could be a code that is sent to you by text message.

Internet browsing history

It is possible for someone to see the websites you have visited by looking through your web browser's history. Clearing your browser history can minimise the chances of someone finding out what you have visited.

Private browsing

The private browsing features offered by web browsers help keep your internet sessions private from other users of the same computer or device. Private browsing modes will not retain your temporary browsing data, browsing history, search records, and cookies, which could otherwise be saved by the web browser.

Apple iPhone settings

Settings on your iPhone can be changed to create a more private and secure device. You can change:

- *Notifications* - allows you to turn off iMessage notifications for anyone who is not in your contacts
- *Previews* - turning off previews will stop anyone from having a glimpse at your notifications – even when the device is locked
- *Location services* - having 'Location Services' turned on means your phone, internet or apps can track where you are. You can disable this by turning your 'Location Services' off
- *Autofill* - your iPhone can store your personal information for AutoFill which makes it easier when filling out forms or logging into an account. It can also make it very easy for a thief to access your accounts if you phone gets stolen
- *Safari* - Settings on your Safari such as 'cross-site tracking', 'block all cookies', 'ask websites not to track you' and 'get warnings for fraudulent websites' can be changed to boost your privacy and security

Android Phone settings

Settings on your Android can be changed to create a more private and secure device. You can change:

- *Location settings* - when you turn off location history, Google stops automatically recording your location
- *Change app permission* - settings for any personal information that can be accessed by any individual app can be changed
- *App installation* - you can stop app installation from unknown sources
- *Two- factor authentication* - To add an extra layer of security on your smartphone, consider utilising two-factor authentication (two-step verification). You can use this sign-in method on any of your accounts
- *Lockdown mode* - If your Android is running Android 9 Pie, 'Lockdown Mode' will lock your device from all Smart Lock and biometric security options. Why would you want to use this technique? Because Lockdown Mode overrides other lock features like biometrics, so someone who forces you to unlock your smartphone with your fingerprint or face still cannot access your Android without your consent

Social Media

We have dedicated guides that can help you secure your social media accounts on the social media platforms listed below; they can be accessed via this link - www.westyorkshire.police.uk/advice/online-crime-safety/online-safety/cyber-crime/social-media-safety


Facebook


Instagram


LinkedIn


Snapchat


Twitter

Is my computer being monitored?

There are tools available that will let an authorised person secretly monitor and record information about your computer. This can be referred to as spyware. It can be installed remotely by dodgy emails and can stay hidden on a computer. It can record and send screenshots, keystrokes typed, web sites visited, emails sent, accounts accessed, passwords typed and more.

Preventing spyware

- Ensure you have anti-virus software on your computer and that you regularly install new updates
- Be wary of dodgy looking emails. Do not open any attachments within them
- If you have doubts that your computer may be monitored, get it checked out by an IT expert

Removing spyware

- Although this may not guarantee complete removal, you could reinstall the operating system
- Replace the hard drive of the computer or purchase a new computer
- Do not copy files or documents from the infected computer onto the new computer
- Use online cloud services to store documents from the infected computer

Is my smartphone being monitored?

Spyware installed on rooted (for Android) or jailbroken (for iPhone) devices can allow someone to turn on the webcam or microphone, take screenshots, see activity on third party apps and intercept, forward, or record phone calls. Almost all phone spyware requires that the person has physical access to the device to install.

Signs to spot on my phone

- Battery draining rapidly and device turning on and off
- Spikes in data usage
- Abuser will know a lot about your phone activity

Preventing spyware

- Because most spyware requires physical access to the phone to install, place a passcode lock on your phone
- Be cautious if someone wants to update or fix something on your phone
- Download anti-virus and anti-spyware apps on your phone
- Android phones have a setting that allows installation from unknown devices. You can turn this off
- The ‘Google Play Protect’ will scan for apps with malware and viruses
- Consider changing your password for your Google Play Store or Apple Store
- Ensure you regularly install the latest software updates

Removing spyware

- If you suspect that spyware is on your device, then use a device that you know is not being monitored
- Consider changing your passwords on a different device and do not access certain accounts from the breached phone
- A factory reset on your phone may remove the spyware. If you choose to do a reset, it is critical that the phone not be connected to the backup to reinstall apps, contacts, photos, etc. this may reinstall the spyware
- Be cautious of reinstalling apps or files from a backup or the App or Play Store as that might inadvertently re-download the spyware app. Manually add the apps or software that you want back onto the phone
- You may also want to take the step of creating an entirely new iCloud or Google account for your device

WEST YORKSHIRE POLICE