A Short Guide to Staying Safe Online

Reduce the risk of stalking and abuse online by protecting your online accounts and devices.

Passwords & 2FA

Strong passwords are essential to securing your online accounts, especially if you use the same password across all of your accounts or if they have been compromised. You should change all of your usernames and passwords across all of your online accounts to be on the safe side. You can use a password manager to help you with this.

Consider using two-factor authentication (2FA) on your most important online accounts as an extra layer of security to prevent unauthorised access.

For more advice on passwords and how to set up 2FA, visit: *https://serocu.police.uk/passwords/*

Smart Devices

Do you have any smart devices in your home that could be accessed remotely and/or could be used to monitor your whereabouts? Keep your smart devices safe by changing the passwords, keeping the firmware updated and monitor the settings in the associated app to restrict access.

For more advice on how to secure your smart devices, visit: *https://www.ncsc.gov.uk/guidance/smart-devices-in-the-home*

Social Media & Digital Footprint

Social media can still be used safely if you secure your accounts using the following top tips:

- Create a strong password and 2FA on all your social media accounts.
- Review devices logged into your accounts in your settings and remove any devices you do not recognise.
- Strong privacy settings are crucial - you want to make sure you are sharing minimal personal information.
- Review your friends/followers - only connect with people you trust.
- Report any abuse to the social media provider.
- If necessary, delete all accounts and create new profiles under a false name.

For more advice on how to use social media safely, visit: *https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely*

Revenge Porn

Revenge porn is where an individual discloses private sexual photos and videos with the intent to cause distress. It is also a criminal offence to threaten to disclose such images and videos. If you feel like you have been a victim of this, you should report it to the Police on 101 or online.

You should also report it to your social media provider, who should be able to help take the post/picture down and help prevent it from appearing elsewhere on the platform.

For Facebook, Instagram and Messenger, visit: *https://www.facebook.com/safety/notwithoutmyconsent*
You can also contact the Revenge Porn Helpline for more advice and guidance: https://revengepornhelpline.org.uk/

Spyware & Location Services

There are different ways a person can follow your movements through your devices. The most common way is via apps such as 'find my friends', GPS fitness trackers or satnav apps. You can minimise this risk by turning off your location services when not you are not using them.

Another way your movements can be monitored is through spyware, which is a type of malicious software that can monitor activity on your devices without you knowing, including stealing your passwords. Anyone that has access to your devices can download it without you knowing. The best way to remove spyware is to restore your device to factory settings and install anti-virus/anti-spyware software.

Keeping your device software and apps updated will also help secure your devices as they patch security vulnerabilities that can be exploited. Turn on automatic updates so you don't have to worry about it.

Internet Browsing & Wi-Fi

When you are browsing the internet using a shared device use 'incognito mode' or 'InPrivate Browsing', which allows you to browse the internet without storing any data that could be retrieved later. Or you can download a private browsing app, which automatically deletes your search history after use.

You can also consider using a Virtual Private Network (VPN), when connected to the internet. A VPN will hide your IP address, which means you will be unidentifiable online. It will also encrypt all of your data so if you are connected to an insecure Wi-Fi, for example in a café or an airport, your data will not be able to be intercepted. If you don't want to use a VPN, avoid connecting to public Wi-Fi and stick to using mobile data.

At home you should consider changing the password to your Wi-Fi router to prevent someone from being able to access your devices via your Wi-Fi network. You may also want to remove/forget any Wi-Fi or Bluetooth connections that may be associated with your ex partner to prevent any unexpected connections.

Further Resources

- Refuge Tech Safety Website: https://refugetechsafety.org/
- SEROCU Domestic Abuse and Stalking Guide: https://serocu.police.uk/cyber-domestic-abuse/
- Women's Aid Online and Digital Abuse: https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/
- General Cyber Security advice: https://serocu.police.uk/individuals/
- Personal Safety App - Hollie Guard: https://hollieguard.com/

Thames Valley Police: Cyber Protect
Email: cyber.protect@thamesvalley.pnn.police.uk
Twitter: @TVPCyber_Fraud