10 Top Tips for anyone who has a partner invading their online privacy:

1. **Social Media:** Ensure privacy settings are updated & maintained. Stalkers can find Survivors by searching name, mobile number or email address (you can remove this search facility) & send friend requests from fake social media accounts impersonating existing friends, hide friend this to avoid this & set privacy settings!
   www.saferinternet.org.uk/advice-centre/social-media-guides
   Additional Tips to consider:
   - **Go for the strongest privacy option available:** For example, if **Only Me**, **Friends** or **Friends of Friends** are the given options you'd opt for **'Only me'.**
   - **Change profile names:** Make being found difficult, but ensure removal of previous associated names. Remove phone numbers & email search options
   - **Approve** who follows you & what you get tagged in
   - **Is it Public?** Before joining seemingly **"closed"** groups, check if the group member's details are open to public before joining. By '**checking in**' you are making your 'check in' post public
   - **What are you sharing?** Think about what **personal** information you are storing. For Example. Storing your full date of birth will only be held against you so why not change your year of birth?
   - **Check contact details privacy settings:** After each App update to ensure they haven't reverted to the default **"public"** setting
   - **Remove unused connected devices:** Remove from your account that aren't required prior to setting up 2FA
   - **Block contacts:** All that link to the stalker & hide friend lists to avoid fake friend requests being sent
   - **Review all above after each social media software update**

2. **Electoral Open Register:** This is where sites like 192.com garner the majority of your personal details and make where you live & other personal information public. **Google yourself** & opt out of anything that links to you. How to Opt out of the 'Open Register':
   www.gov.uk/electoral-register/opt-out-of-the-open-register

3. **Two-Factor Authentication (2FA):** Acts as an extra layer of security. **For more information**: www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa
   How to set up: www.turnon2fa.com/tutorials/

4. **Change security questions:** Online & with your bank as these are the back door to accounts. Avoid facts, use memories or make it up, so long as you remember them that's all that matters!

5. **Passwords:** Change passwords/passcodes to every device within your home & online accounts. Keep it random with 3 random words: www.cyberaware.gov.uk/passwords
   Password Managers: www.ncsc.gov.uk/blog-post/what-does-ncsc-think-password-managers

6. **Restore all devices to factory settings:** Don't back-up/link to your old Cloud accounts, removing risk Spyware previously downloaded. Alternatively get a new device, keeping the old one alive, preventing the stalker from trying to get access to the new one: www.getsafeonline.org/index.php/protecting-your-computer/viruses-and-spyware

7. **Location Services/Sharing:** Turn off location monitoring/GEO tagging on all apps/software/photos/devices used where this isn't required. Delete Apps/software you don't recognise. **Guidance for Android Devices:** https://support.google.com/accounts/answer/3467281?hl=en#5c2f874468c4e **Guidance for Apple Devices**: https://support.apple.com/en-gb/HT207092#5c2f86c64b630

8. **Wi-Fi:** Turn off Wi-Fi & Bluetooth when not required. Use a **Virtual Private Network (VPN)** to protect you on all public WIFI networks. If the stalker has previously been on the home WI-FI then they will automatically authenticate when in range of the home router. Ensure Router password is changed, previously connected devices removed & if possible a firewall installed. **Firewalls:** www.getsafeonline.org/index.php/protecting-your-computer/firewalls/ **Removing people from your WIFI:** www.lifewire.com/detect-and-remove-wi-fi-freeloaders-from-your-network-2487650

9. **Email:** Create a new email account adding 2FA in its set-up, then either update accounts with the new email account information (only after changing passwords/security questions & removing association of the old one) or for best security, set up new accounts with the new email account & delete the old ones.

10. **Browsing without being seen:** Search through sites like the BBC, Wikipedia, then open an incognito browser through the settings option on the right side (where you'd locate your history). Use/Install most secure internet browser, customise your 'Security Settings', use a Password Manager (not "AutoFill" options) to hide what you're browsing.

Additional Cyber Stalking Advice: www.getsafeonline.org/safeguarding-children/cyberstalking1/

Preventing Identity Theft:

- **Get added to CIFAS:** Call **0330 100 0180** (this will cost £20.00). Following specification by the Home Office under the Serious Crime Act 2007, public authorities are able to join CIFAS & share information reciprocally to prevent fraud. For more information visit www.cifas.org.uk
- **Credit Reference Agency (CRA):** A credit score is a tool used by lenders to help determine whether you qualify for credit. You can monitor your credit file activity or report any fraud to a CRA.

  You can also ask for a '**Password Notice of Correction**'. This will put a password on your credit file. We would advise to add the same password to all credit reference agencies, keep this password separate to others & avoid anything the stalker may know. Different lenders use different CRA's for credit applications. This will help to prevent someone from being able to take out credit in your name, but please be aware it is not a 100% guarantee. Delete an email's sent/received requesting a password.