Technology safety & privacy tips

If you have left the abuser consider the following:

Digital Footprint Review: Your digital footprint includes all the information available about you online through your actions or others'.

Review all areas where you use technology and consider updating your security or restricting your visibility where necessary.

Social Media Profiles: Social media profiles contain information about your interests, activities, and social connections.

Update security settings on social media accounts and be cautious about what you share online, including photos and personal information that could put you at risk.

Avoid posting sensitive information such as your home address or phone number.

Online and Digital Safety: Consider if the abuser has accessed your device or online accounts, as they could be compromised.

Consider any connected or joint accounts that may have been installed on multiple devices and could give them access to your information or devices. This could include accounts for iTunes, app stores, Google Play store, Apple ID, eBay, Amazon, Kindle, and others.

Check for spyware and malicious software on your devices regularly.

Be cautious when downloading apps or software from untrusted sources and avoid clicking on suspicious links or opening attachments from unknown sources.

Passwords: It is important to regularly change the passwords on your phone and accounts such as email, Amazon, social networking sites, internet banking, utilities, iCloud, **Apple ID, and Google account**. This should be done even if you don't think that your accounts have been compromised. Additionally, use **two-factor authentication** wherever available to enhance the security of your accounts.

Parental Guidance: If your children use devices set up using your Apple ID or Google account, set up a separate account to prevent abusers from gaining access.

Location settings: It's important to turn off the GPS location settings on your devices to prevent anyone with access to your accounts or devices from tracking and locating you. Review which apps use location settings and turn off any that you don't need, such as 'find my friends/phone/tablet' and fitness trackers.

Email accounts: Your email accounts contain personal information such as your name, address, and contact details, as well as any correspondence you have sent or received.

If you think your email is being monitored, consider creating a new email account on a safer computer/device. Never access the new accounts on a monitored device. When setting up a new email account, don't use any identifying information. Avoid passwords that others can guess.

Secure your home WiFi network: It's possible for someone to access your devices through your WiFi network, even if they're not inside your home. Change the login details and password for your network to prevent unauthorised access.

Be camera aware: Cameras and devices can be accessed remotely or activated by apps. Cover the webcam on your computer/tablet when not in use and check for hidden cameras in or around your home. Trust your instincts, if the abuser knows something that can only be seen, a camera may be used. Reset passwords to devices such as security cameras, video doorbells, and cloud-based voice services such as Alexa.

If you are still living with abuse and/or planning to leave consider the following:

While the technology safety tips provided above can be helpful for those living with abuse, it's important to prioritise your personal safety above all else. It's crucial to assess your own situation and make decisions that minimise any risks to your safety. **Avoid doing anything that could arouse suspicion or increase your risk of harm.**

If you are living with domestic abuse, there are some steps you may want to consider to protect your technology and personal information where you can. Here are some additional technology safety tips:

Clear your browsing history: Clear your internet browser history and cache to prevent your abuser from seeing your online activity. You can do this by entering your browser settings and clearing your history and cache.

Mobile Phone: Delete any texts, messages and call logs you do not want your abuser to see. This can help prevent them from monitoring your communication and whereabouts.

Use a different device: Consider using a different device, such as a computer at a library or a friend's house, to access the internet or a secret phone. This can help keep your online activity private from your abuser.

Be aware of spyware: Your abuser may use spyware to monitor your online activity. Spyware is software installed on your device without your knowledge, allowing someone to track your

keystrokes, take screenshots, and record your conversations. If you suspect your device has been compromised, seek help from a professional.

Disable location tracking: Consider disabling location tracking on your device to prevent your abuser from tracking your movements. You can do this by going into your device's settings and turning off location services **BUT only do this if you are certain it is safe and will not arouse suspicion**. If you believe the abuser is tracking your movements, the safer option will likely be **not to disable this until you are about to flee/leave**. If you need to go somewhere (such as to access support) and you do not want the abuser to be able to track you, think about how you can manage this situation to keep yourself safe.

Change your online accounts: If your abuser has access to your online accounts, consider creating new accounts such as a new email with different usernames and passwords. Make sure to use strong passwords and enable two-factor authentication whenever possible. **BUT** only do this if you have the safe means to do so.

Remember, these tips can help protect your technology and personal information, but they are not a substitute for seeking professional help. If you are in an abusive relationship, consider contacting a professional or **Lincolnshire Domestic Abuse Specialist Service**.