TIPS AND TRICKS

TURN OFF DEFAULT GEO-TRACKING

Strengthen and secure

Be mindful when posting your location. Don't 'check- in' or post photos that may give away your current location. Mobile phones, tablets and some home security systems come with geo-tracking turned on by default. Go into system settings and turn that off. Not only does geo-tracking tell you where you are but it also can tell others when you sleep, the routes you take to work, the stores you frequent and more. It also lets the abuser know when you are most likely to **not** be at home - allowing them easier access. Also go into your usual web browsers settings and turn off location access and history.

ALTER FACTORY PRIVACY SETTINGS

Don't assume it's safe.

Many systems come with automatic tracking, in particular for their own use and to generate income through ads. Go in and double check all privacy settings. Change them to the strictest possible and ensure you use a new password with a combination of letters, capitals, and symbols. Continually change your password and regularly check privacy settings.

SET UP TWO FACTOR IDENTIFICATION

Protect your log-in

If you suspect someone may be monitoring your emails and your accounts, set up 2 factor identification. It may be more work whenever you log in, but if you need to enter a code from your phone to access Facebook on your computer, it is one step the abuser may not be able to complete.

KEEP USING YOUR 'REGULAR' SOCIAL MEDIA

Maintain your presence

If you do suspect someone is monitoring your accounts, keep using them even if you open new ones. That way you can collect evidence and not alert the abuser that you may suspect them. If you do open a new account make sure you do this from a public computer such as a library. Don't use computers that belong to friends or family, where the abuser may have access. Also keep your friend list small; don't add people you haven't personally met. Even if they say they know you.

SMART HOME TECHNOLOGY AND ABUSE

A new pattern of behaviour is increasingly being seen in domestic violence cases; the use of smart home technology and social media as tools of abuse. Internet / WiFi enabled devices, often connected through apps on phones, can be used to intimidate and assert power and control over victims. This invasion of privacy is harrassment, stalking and abuse.

WHAT TO LOOK FOR

- Lights that dim on their own.
- Smart home speakers.
- Automatic pet food dispensers with cameras.
- Smart home A/C and Thermostats.
- Home companions (Google Home, Amazon Alexa).
- Small tracking devices located under cars.
- Security cameras and doorbells.
- Baby video monitors.
- Has someone recently "fixed" your computer?
- Some smart 'plugs' actually have hidden cameras in them.
- Is there a new gadget you don't recognize?

WHAT TO DO

- Install a firewall software program - even on your mobile device.
- Use 2 factor authentication and/or finger print recognition.
- Consider disabling WI-FI on baby monitors.
- Keep any webcams covered with tape.
- Make sure your router is up to date (less than 3 years old).
- Disable remote access to home alarm.
- Use a regular key for your door as opposed to a keypad.
- Avoid **any** online gaming - including any children in the house. This includes games on mobile or tablet devices.
- Password protect every device and log in - use fingerprint technology if available.
- Reset devices by removing the battery - do this regularly.
- Check what devices are connected to your home network by tapping into your router online (use the information on the side of the router - admin URL and password).
- Be aware that Spyware may be on your computer, use a public computer such as library to make searches related to your safety.
- Avoid being on 'others' social media (pictures, posts etc..), such as friends and family, including even your work.

Sometimes old school is better*