Practice guide 4: e-safety checklist

Adapted with thanks from *Northern Territory Domestic and Family Violence Risk Assessment and Management Framework*.

Mobile phone, tablets, computers, smart watches and other devices hold personal information like photos, calendar appointments, call histories, emails and social media posts. Technology-assisted stalking and abuse is more than likely to be used by the perpetrator to monitor and control their partner during the relationship as well as after separation, so it is important to be aware of the risks.

Actions to increase e-safety

- Make sure the victim-survivor is aware that hidden cameras may be installed in their home and that their phone or computer camera may be accessed remotely (through spyware).
- Talk with the victim-survivor about trusting their instincts. If they suspect that the perpetrator is harassing, stalking or monitoring them with technology, it is possible and likely.
- Talk with the victim-survivor and people close to them, including children, to explain the safety risks of posting on social media, such as posting photos that identify where they are.
- Make sure 'location' is turned off on mobile devices.
- Make sure the victim-survivor's devices can't save passwords, or sign in to accounts automatically, and that the victim-survivor can keep login details to all of their accounts safe.
- Help the victim-survivor learn how to delete their history in the Internet browser they use.
- Help the victim-survivor open new private email and social media accounts without information about themselves in the settings, for example profile picture or location.
- Help the victim-survivor to set privacy settings to block others.
- Help the victim-survivor to know how to sign out completely.
- Help the victim-survivor change passwords and PIN numbers (on a safe computer).
- Help the victim-survivor to activate 2-step logins. This is an extra security measure that asks for a security code that is sent via email or mobile, for example mygov website.
- Encourage the victim-survivor to use the Arc app to collect evidence of domestic and family violence safely: https://arc-app.org.au/
- Encourage the victim-survivor to consider their own (prepaid, private) mobile phone and not use their old SIM card. Tell them to handwrite important numbers and manually enter them into the private safe phone.
- Help the victim-survivor to check for unusual apps on their/their child's phone and to delete them if they think it is safe to do so.
- Advise the victim-survivor to switch their device to 'airplane mode' to avoid being tracked.
- Finally, make sure they auto-lock their mobile device with a PIN.

GPS tracking devices are easily available and can be hard to see. They are mostly the size of a postage stamp. Computer spyware is also easy to purchase and install on home computers, devices, smartphones and watches. This allows the perpetrator to track and access what the victim-survivor is doing and seeing. A device or smart watch can also be turned into a GPS tracking tool and a listening or recording device.

Often, the victim-survivor wants to stop the stalking behaviour by getting rid of the technology. However, this could escalate the controlling and dangerous behaviour if the perpetrator feels they are no longer in control. Workers should think about what might happen if the victim-survivor removes the device. Another option could be for the victim-survivor to use a safer computer and/or device whilst keeping the one being monitored

Signs someone is being monitored

- Does the perpetrator seem to know the victim-survivor's location?
- Has the victim-survivor noticed any strange activity on their phone?
- Does the perpetrator have access to the victim-survivor's mobile phone, social media accounts, bills or passwords?
- Does the perpetrator know what the victim-survivor is doing when they are home alone?
- Does the perpetrator seem to know where the victim-survivor goes even when they don't have their mobile? It might not be their mobile that is revealing the location, it could be a GPS tracker or other technology.
- Does the victim-survivor experience a quick battery drain or a spike in data usage on their mobile phone? This can indicate that spyware is running on the phone.