Protecting clients from technology-facilitated abuse

A guide to support clients **wanting to use technology safely**

Client profile

- Has left their abuser
- Wants to safely reconnect with technology
- Has time and headspace to comprehensively review each device, account and app

Goal

- Empower them to use technology and their devices safely and reduce the risk of technology-facilitated abuse

Objectives

- Help them understand how technology can be misused by an abuser
- Reinforce that taking these steps will reduce the risk of technology-facilitated abuse but does not eliminate it
- Support specific steps across devices, accounts and apps that will help them to use technology more safely
- Discuss signs that could suggest their devices have been compromised by spyware

Key safety requirements for frontline workers to consider

- Any technology safety planning is done in the context of broader domestic, family and sexual violence risk assessment and safety planning tools.
- Any changes to technology and device use are only made after considering your client's specific situation and safety.
- Please be aware their abuser might be alerted to changes made to their (or any children's) devices or technology.

7 technology safety steps to work through with clients

1. Explain the role of technology-facilitated abuse

- When digital technology (the internet, devices, smart technology) is used to harm or abuse someone, it's called 'technology-facilitated abuse' or '**tech-based abuse**'.
- This form of abuse occurs in most cases of domestic and family violence.
- This form of abuse can be covered by court orders, such as an Apprehended Domestic Violence Order.
- The abuse includes controlling the use of someone's technology and devices and using technology to scare or shame them.
- Some types of abuse are more obvious, such as **harassment, threats**, impersonation.
- Some types of abuse are more hidden, such as **surveillance and tracking**.
- Children's devices can also be used to track and cause harm – for example using tracking apps on phones or tablets, or cameras in toys.

2. Conduct a technology, device and account audit. (Refer to: **Technology audit: Identifying a client's devices, apps and online accounts**). This audit can support both current and future safety planning.

3. Identify their most vulnerable devices, apps and online accounts

Base your assessment on whether:

- location details can be tracked or shared
- locations can be tagged
- sensitive or personal information is stored
- an address is required
- the abuser had access, or is likely to have had access, to specific devices, accounts or apps.

4. Recommend these safety steps for smart devices, especially any identified in step 3:

- If possible, reset devices to factory settings. If not possible, **reset passwords/ passphrases** or passcodes across all devices. After doing one or other of these:
  - avoid linking to any previous accounts such as Google Drive, iCloud, Dropbox
  - avoid reinstalling the phone from a backup.
- Call the mobile phone provider and put a verbal password on the mobile account to prevent 'SIM swapping'. 'SIM swapping' is when someone else takes control of your phone by tricking your carrier to connect your phone number to a SIM card in their possession.
- Set up facial/fingerprint recognition wherever possible.
- Review privacy and security settings and set to most secure.
- Make sure **location sharing is off**.
- Turn off bluetooth when not using.
- Turn off iCloud, Google Drive and other automatic drive or data backups.
- Identify any unused, duplicated or unrecognised apps or software. Before deleting these, consider whether to use them as evidence of technology-facilitated abuse.
- Update the operating system's software.
- Set software updates to install automatically.
- Make sure SMS forwarding is not set up on any devices.
- Install anti-virus software to help detect spyware.
- Consider covering cameras with removable tape or a sticker when not using them.

5. Recommend these safety steps for online accounts and apps, especially any identified in step 3:

- For high-risk accounts, consider creating new online accounts. If not possible, reset passwords/passphrases or passcodes.
- If possible, enable multi-factor authentication with the new phone number or new email.
- For every online account, review and upgrade privacy and security settings when possible.
- For any online apps that require a location (for example, food delivery, ride share), only activate location data settings when using the app.
- Call major government and service providers (such as Centrelink, Medicare, banks, phone services) and ask what additional security steps they can take to protect online accounts.
- Limit the amount of location data shared via online accounts or online posts, especially on social media.

6. Let them know devices may be infected with spyware. Here are some signs:

- A device is slower than usual or takes a long time to load.
- A device is switching itself off and on.
- There are unexplained spikes in data use.
- Apps, emails or messages are unexpectedly deleted.
- The device is unable to call certain numbers or access certain websites.

7. Recommend they speak with any children in their care about the importance of the following online safety measures:

- Avoid sharing or posting photos, videos or backgrounds that could identify their location (for example, street signs, landmarks, school uniforms) on social media, gaming or video calls.
- Avoid checking-in at venues on social media.
- Avoid tagging family members online.

Need help to support your client?

Request a call back from eSafety's Technology-Facilitated Abuse Support Service via the enquiry form.

For resources and online safety advice, visit: eSafety.gov.au/TFA-support-service