Protecting clients from technology-facilitated abuse

A guide to support clients thinking about leaving their abuser

Client profile

- Thinking about leaving their abuser
- Their safety depends on not alerting their abuser to their plans to leave
- Open to making changes to technology and device use as part of their safety plan

Goal

- Reduce current and future risk of technology-facilitated abuse without triggering an escalation in control or violence

Objectives

- Help them understand how technology can be misused by an abuser
- Help them access a safe phone or safe device
- Support them to take steps to reduce future risk of tracking and surveillance

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.
- In some cases, it may be safest not to make any changes to their device or technology to avoid triggering further violence.

8 technology safety steps to work through with clients

1. Explain 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. Help them access a safe phone or safe device for sensitive communication

A safe device is:

- new (**Wesnet provides new phones via the Safe Connections Program**), or borrowed from a trusted person and is a device their abuser has never accessed
- not linked to or backed up by an existing device
- not linked to or backed up by any current iCloud, Google, Outlook or other online accounts.

Before using a safe device, recommend:

- turning off **bluetooth, wi-fi auto connect and location services**
- downloading a subscription-based VPN ('**virtual private network**') before using wi-fi.

There are other options if accessing a safe device is not possible:

- Reset current device to factory settings.
- Use a work computer (if it's safe to do so) or go to a library or a trusted person's place to use their computer.

Across all devices, recommend they browse in **incognito** or InPrivate mode and log out of any online accounts they have logged into.

3. Agree on a plan for hiding and using the safe device

Recommend hiding the safe device or phone somewhere their abuser cannot access.

- Use the safe device for:
- emergency calls and any calls related to a safe exit
- safety planning and research
- setting up new accounts / apps that are part of the safety plan
- collecting evidence of abuse for possible future court cases (see step **6**. **Discuss what evidence they might like to collect on their safe device**).

So as not to alert their abuser, recommend they continue using their known device as much as possible for:

- planning and communicating non-sensitive information to family and friends
- regular day-to-day business that won't impact on any safety plan.

4. Conduct a technology, device and account audit. (Refer to: **Technology audit: Identifying a client's devices, apps and online accounts**). This audit can support current safety planning (see step 5 and 8), as well as future safety planning.

5. Identify important new accounts to set up safely and securely to support a plan to leave, including:

- email accounts
- travel card accounts
- online bank account and credit card
- MyGov, including Centrelink and Medicare.

6. Discuss what evidence they could collect on their safe device

This might include:

- notes of dates and times of repeated harassing or abusive behaviours
- screenshots, photos and recordings
- notes of any suspected or observed monitoring or stalking activities.

Other options:

- If accessing a safe device is not possible, evidence can also be stored on a USB or hard drive. In this situation, it is best to store the USB or hard drive in a safe place their abuser cannot access, such as a trusted friend or relative's home. Also, recommend not plugging any personal device into a computer their abuser uses or can access.

7. Discuss what might need to happen once they leave their abuser

This might include:

- temporary restricted access to their smart devices, including wearables, to avoid risk of tracking and surveillance
- comprehensive review of all devices and accounts to improve the safety and privacy settings, including those used by any children in their care.

8. Recommend these extra safety steps:

- Update device passwords/passphrases and activate facial or fingerprint recognition.
- Update email passwords/passphrases and ensure mail forwarding is not set up.
- Update social media passwords/passphrases and account verification.
- Identify any unused, duplicated or unrecognised apps or software. Before deleting these, consider whether to use them as evidence of technology-facilitated abuse.
- Update operating software across devices.
- Set software updates to install automatically.
- Install anti-virus software to help detect spyware.

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