Tech abuse: Client conversation starters & safety planning

WESNET
The Women's Services Network

How to use this resource

This resource is to help SADFV practitioners discuss tech abuse with their clients from culturally and linguistically diverse or Aboriginal and/or Torres Strait Islander backgrounds. The resource contains question prompts, tech safety strategies and handout links.

The companion resource—a printable PDF 'Is Tech Abuse Happening to You?' poster—is available in English (A3 & A4) and several other languages

Download the poster at https://techsafety.org.au/tech-abuse-posters/.

Tech abuse is a common tactic of perpetrators of abuse. If your client has experienced tech abuse, it should be considered carefully in her safety plan. ***Threats and stalking should be taken seriously.***

Note: The following tech safety strategies may not suit every situation.

Does someone control, take, break, or make you share your phone?

- Do you have your own phone? What do you use your phone for?
- Does someone keep you from talking to your family or people overseas?
- Do you share your phone with someone else or does someone else look at your phone?
- Have you ever needed to use your phone but could not use it? Can you tell me more about what was going on?
- Does anyone know how to unlock your phone or do they make you unlock it?

What to do

- Consider using a 'safe' phone (new phone or trusted family/friend's phone) for safety planning activities, or leaving it with trusted family/friends.
- Use the phone as normal, however find another way that is safe to talk or write about private things or safety planning.
- Let people know when you see them that your phone is not private. Use a code word that can let the other person know if someone is listening to your call or reading your texts.
- Write down the numbers of people on your phone and hide them in case your phone gets taken or smashed.
- Plan a regular time to call a friend or support worker. Let them know what you would like them to do if they do not hear from you.
- If it is safe, ask a neighbour to call 000 if they hear or see a sign like your curtains pulled down.
- Find more info at techsafety.org.au/resources/resources-women/. Handouts include 10 Steps to Maximise Privacy, Increasing Privacy and Security When Using Google, Online Privacy and Safety Tips.

Does someone access, control, or lock you out of your accounts (email, banking, myGov etc)?

- Do you share accounts with someone? Do they set it up or make decisions for you about your account?
- Can someone go into your email accounts, bank accounts, myGov, ImmiAccount, Google Account, GooglePlay, Apple ID or iCloud account?
- Are the things you do on your phone or accounts private or does someone else see them?
- Does someone know your passwords or go into your accounts?
- Has someone ever locked you out of your accounts or made changes to them?
- Does someone make accounts in your name or lie about you wanting an account?
- Do you have your own bank account or do you share one with someone?

What to do

- Use a long password that is hard for someone to guess, and use 2-step verification or multi-factor authentication if safe to do so.
- Use a different password for every account.
- Consider changing account passwords or contacting the agencies to set up a new account.
- Setup new 'safe' accounts on a safe phone or library computer. Use those accounts only on a device the abuser does not use.
- Find more info at techsafety.org.au/resources/resources-women/. Handouts include Password Safety, Tips for Secure Email, 12 Safety Tips for Smartphones, Being Web Wise.

Does someone shame, humiliate, threaten, or impersonate you using social media apps text, email, or phone?

- Does someone say bad things about you on social media?
- Do other people start saying things to hurt you or 'like' mean things about you that someone said?
- Does someone make you feel afraid to use social media? What do they do?
- Has anyone tricked you or acted like they were you or someone you know on social media?

What to do

- Keep social media posts, who posted them, and who received them (use the 'download data' feature, copy, screenshot, take a photo with another 'safe' device, print, USB).
- Adjust security and privacy settings (including tagging) on social media apps. Block the abuser if it is safe to do so.
- These behaviours may be against the law and help can be sought from a lawyer or Police.
- Find more info at techsafety.org.au/resources/resources-women/. Handouts include Facebook Privacy & Safety: A Guide for Survivors of Abuse, Privacy Considerations When Posting Content Online, Safety & Privacy on Twitter: A Guide for Survivors of Harassment and Abuse.

Tech abuse: Client conversation starters & safety planning

WESNET
The Women's Services Network

Does someone harass, abuse, punish or threaten you via text, communication apps (WhatsApp, Viber, Skype, FaceTime), email or phone?

- Has anyone said things using a phone to hurt you or scare you?
- Do you have to do things with your phone so you do not get in trouble?
- Does someone send you messages all the time or get angry if you do not write back?

What to do

- Write down what was said in phone calls and keep the call history logs, sometimes called 'recents' (screenshot, take a photo with another 'safe' device, print). Call history and text logs can also be accessed through mobile providers.
- Keep the text messages (copy, screenshot, take a photo with another 'safe' device, print, USB).
- Swipe Wi-Fi and Bluetooth off and then switch the device to 'Flight' or 'Aeroplane' mode to preserve the call and text messages on the device.
- Take the device and any copies, screenshots, printouts, USB to your lawyer or police to have evidence formally documented, as these behaviours may be against the law.
- Find more info at techsafety.org.au/resources-women/. Handouts include Dealing with Harassing Calls, Texts and Messages, Technology Safety Plan: A Guide for Survivors and Frontline Workers, Documentation Tips for Survivors of Technology Abuse and Stalking.

Does someone share or threaten to share images without your consent (image-based abuse)?

- Has someone taken private photos of you with or without your consent?
- Have they shared those photos or said that they will share them?
- Did they say these things to you in person or send them to you?

What to do

- Ask for the person to take the image down and delete it.
- Talk to someone you can trust like a counsellor from a local agency or 1800RESPECT.
- Report to the social media company, police and/or the eSafety Commission.
- Sharing of intimate images without consent may be against the law and help may be sought from a lawyer or Police.
- Find more info at techsafety.org.au/resources/resources-women/.
- Handouts include Image-Based Abuse, and Women's Legal Guides.

Tech abuse: Client conversation starters & safety planning

WESNET
The Women's Services Network

This resource was created to better support women experiencing tech abuse who identify as Aboriginal and Torres Strait Islander and/ or culturally and linguistically diverse. These groups experience DFV at significantly higher rates than the Australian population overall and have unique barriers to accessing support. It was developed in response to DFV practitioner recommendations for more targeted resources during WESNET's National Listening Tour of urban and regional specialist women's services. View the report at https://techsafety.org.au/resources/practitioner-resource/.

Does someone know where you are, what you do, or stalk you, using location/GPS tracking, monitoring, spyware/ or keystroke logger apps, or hidden camera?

- Does someone use your phone to watch you or know where you go?
- Does someone know things that you have not told them? How do you think they found out about this?
- Does someone seem to know some things but not others? What are the things they know? Where does that information 'live'?
- Do weird things happen with your phone, car or home that do not make sense?
- If your client suspects her location is being monitored, or if she is being stalked, her device, home, car, belongings or her children's device or belongings may be compromised.
- ***ALL STALKING SHOULD BE TAKEN SERIOUSLY***

What to do

- Consider using a 'safe' device (new phone or trusted family/friend's phone) for safety planning activities and/or leaving it with trusted family/friends.
- Figure out if there is a pattern related to what someone knows. Do they know where you go all the time or just when you drive your car or use public transport?
- Discuss how much detail someone knows about you to narrow down how and where they get information. Do they only know certain things or do they seem to know everything? Consider mapping what they know and where it 'lives'.
- Check global location settings on the phone and for each app as some apps may collect and share location information.
- Stalking behaviours may be against the law and help can be sought from a lawyer or Police.
- Find more info at techsafety.org.au/resources/resources-women/. Handouts include Smartphone and Location Safety Strategies, Mobile Spyware: Identification, Removal and Prevention, Android Privacy & Security Guide, iPhone Privacy & Security Guide.

Questions?
Contact safetynet@wesnet.org.au

More information and handouts
https://techsafety.org.au