eSafetyWomen

Technology-facilitated abuse Safety assessment checklist

How to use the checklist

This checklist can be used to assist in your client's safety plan. Refer to the eSafetyWomen website esafety.gov.au/women and the hyperlinks in the electronic version of this document for more information.

Quick fixes for technology-facilitated abuse
If your client is at risk of technology-facilitated abuse, it is important not to react without first considering possible implications. Removing an online presence or discarding devices could alert an abuser and may escalate abusive behaviour if they think their ex-partner is removing control and access.

A client who has no devices and removes herself from social media may be safer in the short term. However, longer term this could generate other issues such as isolation from friends, family and sources of support, as well as practical things such as the inability to job search.

The following list of quick fixes and good technology hygiene is not intended to be exhaustive. Rather, it should be read as a series of possible safeguards.

Quick fixes and good technology hygiene

Keep an eye out: look for signs that may indicate you're being monitored or tracked.
Use safe devices at community houses, libraries and women's services.
Get a new email address that isn't linked to your name, using a safe device.
Use a new email address to sign up to any accounts so bills don't reach your abuser.
Use different screen names and usernames for different platforms.
Ditch your device or use an old device.
Get a new device with a new carrier where you are the only account holder.
Don't switch sims but re-enter all data on any new devices.
Consider going prepaid and pay with cash.
Use a friend's or family member's device that the abuser will not check.
Put passwords/passcodes on all devices.
Change existing passwords/passcodes.
Check all your devices settings (Disable Bluetooth, location-based services, apps and GPS).
Cover or disable cameras and search for hidden ones.
Run anti-malware and security software.
Learn how to block your number if you need to call the abuser.
Talk to friends and family and remind them not to tag you, check you in or post about you online.
Make sure your settings on social media are private and know how to get help on these sites to stay secure.
Delete your browsing history regularly or use private browsing.
Always log off or sign out of social media, billing and email accounts.
Provide copies of court orders to every Government agency you use, myGov, banks, schools, childcare, kindergartens and preschools, sporting clubs and everywhere your child attends and consider becoming a silent elector.
Contact agencies (such as doctors and hospitals) that may have your abuser listed as "next of kin".

Technology-facilitated abuse Safety assessment checklist

eSafetyWomen

✓ **Immediate safety plan required**

✓ **Safety plan recommended**

Risk Indicator		Yes
1.	Is the abuser or his family or friends technologically savvy or working in a technology-related industry?	☐
2.	Do you believe that the abuser is monitoring any of your devices?	☐
3.	Does the abuser seem to know a lot about what you are doing and places you visit?	☐
4.	Could the abuser have intimate photos of you?	☐
Phones, tablets, laptops, desktops, webcams		
5.	Has there been anything unusual happening with your device (strange apps, increased battery drain, unknown programs operating in the background, slower speeds)?	☐
6.	Has the abuser had access to any of your devices?	☐
7.	Does your abuser, or your children know your passcodes or passwords?	☐
8.	Are your GPS and location services on? Do you use any location apps or have the "Find my iPhone", "Locate my phone" or "Frequent locations" features enabled?	☐
9.	Have any of your children received a device from your abuser?	☐
10.	Do you think your children's devices are being monitored?	☐
11.	Do you have Family Sharing or the Windows equivalent enabled?	☐
12.	Is Bluetooth enabled on your device all the time?	☐
13.	Is your malware protection out of date?	☐
14.	Do you leave your webcam or Smart TV camera uncovered when not in use?	☐
Social media		
15.	Are your privacy settings unrestricted?	☐
16.	Do you display personal information online (eg. your actual name or the suburb where you live)?	☐

Safety assessment checklist cont...

Social media continued		Yes
17.	Are your children on social media?	☐
18.	Do your children share personal information with others online?	☐
19.	Do friends and family or colleagues tag you on social media or check you in?	☐
20.	Do you have an online dating profile?	☐
Online transactional accounts		
21.	Does the abuser know your ATM PIN?	☐
22.	Do you use the same password for all your accounts?	☐
23.	Do you have an eToll, eTag e-Pass or go via pass linked to an account?	☐
24.	Do you have a public transport card or parking card linked to an account?	☐
25.	Do you have a joint banking account?	☐
26.	Do you use online banking?	☐
27.	Does the abuser know your username and password?	☐
28.	Is your credit card linked to accounts like iTunes, Google Play Store or Ticket agencies?	☐
29.	Do you receive email communications jointly with the abuser (e.g. emails from your child's school, strata reports)?	☐
Other devices		
30.	Does your abuser have access to your cars inbuilt navigation system or stand-alone GPS?	☐
31.	Did your abuser set up your CCTV?	☐
32.	Is your car connected to the internet, eg via an in-car entertainment system?	☐
33.	Do you have a baby monitor, home alarm system, or physical activity tracker like a Fitbit?	☐