TELSTRA SAFE CONNECTIONS

IT'S HOW WE CONNECT

A partnership with WESNET to help women impacted by domestic violence to stay safely connected.

Mobile phones, tablets, computers and other devices hold lots of personal information including photos, calendar appointments, call histories, emails and social media posts.

The Apps or software installed on your device can potentially allow others to access your personal information and location, particularly if you have previously shared account or sign in information. There are simple steps you can take to protect yourself and your device.

Important: if you think an abuser has accessed your device put it into 'flight mode' now.

5 TIPS TO PROTECT YOURSELF AND YOUR MOBILE PHONE

1. Lock your mobile with a new password. Don't share your password with others.
2. Turn location/GPS and Bluetooth off when not required. Some Apps may request access to your location when you first download them. Decline wherever possible or if you do not need to access the location service of the App.
3. Install security software and run antivirus updates. Regularly review the Apps on your phone and delete those not in use.
4. Be careful about what you post on social media. Don't post anything that reveals your location.
5. Before discarding your old handset, save all harassing/threatening texts and voicemail messages as evidence. Print screen shots and text messages.

If something feels wrong – trust your instinct. Research shows that abusers often misuse technology to stalk and control victims.*

If you are in danger call 000, and 1800 RESPECT (1800 737 732) for counselling and access to support services.

SAFETY TIPS FOR REPLACING YOUR MOBILE PHONE

- Be careful moving data from the previous mobile onto the new handset. The safest method is to manually input contacts and be sure to use a new SIM card.
- Remember that when you switch 'flight mode' status off on a monitored mobile, a stalker may be able to locate you.
- A stalker may escalate abusive behaviour if he/she suspects you are removing access to monitored technology. If your device is monitored it may be safer to keep using it for harmless activities, such as reading the news.
- Use your new handset to research an escape plan, and contact support services.
- Don't provide anyone access to your new mobile phone or your password.

SIGNS YOU ARE BEING MONITORED

- Does the person seem to know your location whenever you have your mobile with you?
- Have you noticed any unusual activity on your phone? Excessive battery drain or a spike in data usage can indicate that spyware is running on your mobile.
- Does the person have access to your mobile phone, social media accounts, bills or passwords?
- Does the person know what you are doing when you are home alone? There may be hidden cameras in your house. Check gifts given to you from the abusive person and think about which room you are in when the person seems to know what you are doing.
- Does the person seem to know where you go even when you don't have your mobile? It might not be your mobile, it could be a GPS tracker or other technology.

TAKE ACTION

Change all your user names and passwords regularly

This includes social media services, apps and all devices.

Create a separate email account for safety planning and legal communication and only use this on a safe, non-monitored device.

Managing violence and abuse on your own is very dangerous

Work with a victim advocate (domestic violence or sexual assault support worker) to help you plan for safety.

Always call 000 in an emergency.

Document behaviour

Take all threats seriously whether verbal or text.

Save texts, print your call history and take screenshots.

Take the device to the police, your lawyer or community legal service to have the evidence documented.

Use technology carefully

Be aware that someone could be using multiple devices to monitor you.

Narrowing down a source will help you to create a safety plan.

Adjust your children's privacy settings on devices and social media

Talk to your children about how they interact online.

If you have a parenting plan or court order talk to your child about when and how the other parent is allowed to communicate with him/her.

Instruct your child to notify you and save the history if unauthorised communications are received.

Warn friends and family - they may accidentally reveal your location. Innocent comments can provide clues about your location.

THINGS YOU SHOULD KNOW

Are you sharing too much information?

Geo tags, posts and photos provide clues about your location, home address and movements, potentially putting you at risk. Regularly check your privacy settings as social media sites may change their policies.

Spyware and other methods for monitoring

There are many applications and programs that can be used for stalking and monitoring. If you are concerned about spyware on devices have them checked by a computer expert or the police.

Spyware: Software that can gather information about a user's activities online and may send such information to another entity without consent.

Blue bugging: Using a Bluetooth connection to access a user's phone including visibility of messages, call history, photos and contact list.

Key Logging: Software that can log every letter and character typed into a key pad. It can capture passwords, codes and communications.

Be aware that software can be installed remotely without your knowledge

It is usually done 'behind the scenes' when a seemingly ordinary file, such as a photo, is opened or downloaded. Again, if you think you are being monitored, trust your instincts and seek help from a support advocate.

GET HELP

Important: In an emergency call 000.

Call 1800 RESPECT (1800 737 732) to get help with safety planning and find support for dealing with violence and abuse

or

access online counselling at
www.1800respect.org.au

Safety resources:

www.wesnet.org.au

www.telstra.com/cyber-safety

WESNET
The Women's Services Network

Acknowledgments and references: WESNET, Safety Planning Around Technology: A Guide for Survivors of Domestic Violence or Dating Violence NNEDV Technology Safety Plan: A Guide for Survivors and Advocates
** Woodlock, Delanie (2014) Technology-facilitated stalking: findings and resources from the SmartSafe project Domestic Violence Resource Centre Victoria, Collingwood.*