

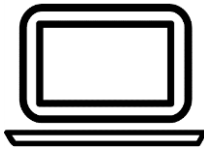
PASSWORD CHECKLIST

- Use this list to think about what passwords you need to change
- Make sure you keep this list somewhere safe
- Make sure you change your password using a safe device
- If you don't know how to change your password, Google it on a **safe device** or ask a trusted friend, family member or social worker to help you
- Try to set up two-step verification to help secure your App & email accounts

Your devices

Also consider your children's devices

Computer



Phone



Tablet



Make sure your devices are password/PIN/print protected with a strong password

App Store



Google Play



Windows Store



Galaxy Store



App Accounts

Your log in details for App accounts allow built-in Apps like "Find My Phone" to track you remotely using GPS. They can also be used to set up remote spyware. Change your password or turn off location settings

Apps, social media & messenger accounts

Facebook



Google+



Instagram



LinkedIn



These are suggestions – check what Apps are on your device

Online forums



Pinterest



Twitter



Apps like Whatsapp & Messenger are linked to your phone & can't be password protected. Consider deleting or getting a "chat lock" App

Delete Apps you don't use or don't recognise

Snapchat



Uber



Skype



Games



Email

Gmail



Outlook or Hotmail



Yahoo



iCloud Mail



iCloud

- Set up a new email address on a safe computer. Don't use any identifying features in this email address (e.g., your name, year of birth).
- Check your email address to ensure "mail forwarding" has not been activated. See www.esafety.gov.au/women for videos on how to check "mail forwarding" settings.
- Consider deleting in-built mail Apps on your device if another person has access to that device.

Government accounts

Centrelink



MyGov



Opal



E-Toll



Think about security questions on government accounts & whether to change them

Online shopping

PayPal



ebay



Flights



Groceries & shopping



Cloud storage

iCloud



OneDrive



Dropbox



Google Drive



Cloud storage may automatically back-up information from your devices (for example, Dropbox may ask to save photos when you plug an Apple device into a computer). Check your settings.

Utilities

Online banking Apps



TV accounts



Fitness Apps



Internet & phone accounts



IMPORTANT INFORMATION ABOUT PASSWORDS & INTERNET BROWSERS!



- Saved usernames & passwords can be accessed & viewed on most browsers.
- Do **not** click "save my password" to ensure your passwords are not viewable or use **private browsing** so your search history & passwords are not logged.
Eg, Chrome: Incognito, Internet Explorer: InPrivate, Firefox & Safari: Private browsing.
- Learn how to delete saved passwords by Googling your browser name (eg, Chrome, Safari, Internet Explorer) & "delete saved passwords".

HOT TIPS FOR STRONG PASSWORDS

- Use different passwords for different sites/accounts/Apps.
- Consider using a master password account, eg, **LastPass**...
- Don't use personal details like your name, birthday, child/pet names or obvious passwords like sequences (eg, 1234, qwerty) or "password".
- Try three random words together, eg, "goose", "blanket", "burrito" = gooseblanketburrito.
- Add numbers, Capitals, symbols for extra strength, eg, Gooseblanketburrito99!
- Make sure your passwords are at least 8 characters in length.
- Don't write down your passwords where they can be found.
- Be careful of websites that are linked with a single sign in. Eg, signing into YouTube may also sign you into Gmail, Google+, Google Drive, Google Maps, etc.
- Always log out & close Apps when you are done.



Learn more & watch videos about online safety at www.esafety.gov.au/women

For free legal advice about technology-facilitated stalking or abuse, call the **Domestic Violence Unit**, Legal Aid NSW on **(02) 9219 6300**