Computer and Laptop Security Tips

techsafety.org.au

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of October 2025.

Computers and laptops are highly capable and adaptable devices that can power everything from smartphones to household appliances. Many are already integrated into our daily lives, and transition easily between the household and work or school. With the development of technology, computers now are capable of not only computing capabilities, but communication as well.

Computers can be vulnerable to exploitation by domestic/family violence abusers to gain information about a survivor's location, activities and communication. While a computer may not contain as much intimate communication as a smartphone, it still contains a lot of personal information including email accounts,web browsing activity, forms that have been completed, and documents along with other stored information. Whether you're setting up a new computer or just reviewing your computer's settings, we have provided here some privacy and security tips to protect you.

Good Practice for Computer Security

Put a password on your computer

Locking down your computer with a strong passphrase is the first thing you can do to prevent unauthorised access to your devices. We recommend updating this password periodically and not re-using passwords or codes. For more information about creating a strong password, review our Passwords Handout.

Don't click on unknown or suspicious links

Another good practice is not to click on links or attachments from suspicious senders or websites. Because malware can sometimes be embedded in these links or attachments, "opening" one could install the malware.

Log out of accounts and quit programs

When you finish using an online account, a program on your computer, or even the computer itself, log off and close the account. Leaving accounts and your computer logged in could make it easier for someone else to get into your accounts. Even if you don't think someone has physical access to your computer, it's always best practice to log out when you've finished.

Adjust device settings and permissions

Turn off WiFi, Bluetooth, Airdrop, or other connectivity access on your computer if you're not using it. If permissions have been turned off or are set to limited access, it will be harder for someone to connect with your device remotely. You can always turn it on again when you need to connect.

Configure Directory Account

The majority of computers require a directory or principal account to manage the devices data, security, software and connected tools. This is a great first step to take to strengthen the security and protection of your device. This account may be in the form of a centralised cloud account, such as an Apple, Google or Microsoft account or it may be a local account, which is centralised only to the device and the information within that. Depending on the account, you can adjust settings to improve privacy and security such as turning off location services, turning on automatic software updates and autolocking the device after a certain period of inactivity.

Utilise software security

Software security are products that are built and maintained to protect your devices and networks from external attacks. Examples of software security include firewalls, antivirus software and email security tools. Many of these tools are incorporated into programs, however there are third party products available to address any additional security gaps that you identify. We recommend conducting research on what software is most suitable for your needs and network before downloading and installing anything to your system. Be aware of free or heavily discounted software as it may download unintended malware.