Online Privacy and Safety 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 July 2025.

Safety and privacy is a concern for many people when browsing the web or engaging with online accounts, apps and other digital platforms. A good general rule is to engage in online activities with the understanding that anything and everything you do may become public. Another general rule is that you can't be completely anonymous online. However, you can take steps to prevent sensitive and personal information from circulating on the web.

Safe Web Browsing

Safe web browsing encompasses tools and practices that you can implement to enhance your online privacy and security while browsing the web and using web-based applications.

- Use a private browser or enable incognito mode when browsing online. This will ensure that your browsing history, cookies, log-in sessions, and site data are not saved or recorded.
- Periodically clear your cache; this will delete temporary files stored by your browser.
- Delete browser history, cookies, temporary internet files and saved forms and passwords from your web browser often.
- Keep your browser and any plug-ins up to date, and conduct thorough research on your privacy and security before installing browser extensions.
- Block pop-ups and use an ad blocker and a Virtual Private Network (VPN).
- Consciously log out of accounts before closing your browser.

Setting Up Accounts

Nowadays, we are required to set up accounts for a range of products and services. A lot of accounts are also categorised as web applications, meaning you can access the same account through a web browser or have the same account on applications across different devices. This means that the accessibility of the account is significantly broader compared to single sign-on accounts.

General account privacy and safety tips

- Consider whether setting up the account is necessary, what information it requests, and if there is an option to continue as a guest user.
- Always read the terms and conditions or Terms of Service (TOS) of the account before signing up. Review the privacy and security measures, as well as consumer data protection.
- When setting up accounts that may contain personally identifiable information (PII), avoid using compromised networks or public Wi-Fi. If required, use incognito/private browsing or a Virtual Private Network (VPN).
- When setting up new accounts, do your best to keep them isolated from compromised devices or accounts. This includes recovery settings, such as Multi-Factor Authentication (MFA).

Setting up email account

- Have more than one email account and use them for different purposes.
- Consider using an end-to-end encrypted email service provider or encryption software to enhance your email privacy.
- Create email addresses that don't include identifiable details such as your name, your children's names, your pet's name, nicknames, significant dates or numbers.
- Secure the account with two-step verification or multifactor authentication, along with a long and strong passphrase.
- Turn off automatic image downloading on both your computer and devices.
- Limit the use of the 'forwarding' feature, as you may be exposing the email content (and all of those in the communication chain) to other servers that may be unsecured and unencrypted.
- Set expiration dates on emails so that they will no longer be readable by the recipient, or anyone else, after a specific date.
- Store email records securely offline on an external hard drive or in a paper file if they contain sensitive details or are important for documentation or evidence purposes.
- Delete email copies and have the recipient do the same if it's not safe to have copies accessible online.
- Delete email correspondence you no longer need or want, and ensure it is emptied from the trash.

Setting up Social Media and other accounts

- Where possible and if desired, set up accounts as private rather than public. This will limit who can see your content and enhance privacy.
- Utilise the privacy settings and tools available; depending on the account, you may be able to hide your account as discoverable. Access the help centre or support centre for the application.

- Turn off or manage permissions, such as location information, microphone, and camera access, and limit access to the camera roll and photos. This may be accessible across the account settings and the device settings.
- Ensure recovery settings are secure, including recovery details and setting up login alerts.
- Manually log out of accounts on both web and mobile applications.
-

Password Management

Alongside the rise of accounts required to manage and use services today, the majority of these accounts also need a password. That is a lot of passwords to manage and set up. Below are some tips to enhance the privacy and safety of your passwords.

- The safest passwords are passphrases! This is a combination of words (ideally 4-5) with symbols, numbers and capitalisation. Misspellings of these words can make the password more secure because it is much harder to crack a password when it is not grammatically correct. Passphrases are much more secure than traditional jumbled passwords and are easier to remember.
- Try not to have the same password for every account. Develop a system that's easy to remember but allows you to have a unique password for each account.
- Streamline your password management by keeping it private and individualised. It may be safest to write them down and keep them on you at all times, or it may be best to use a reputable password manager. If possible, keep your essential passwords memorised and unrecorded.
- When setting or updating passwords, ensure you are doing so on a secure device and a safe network.
- Update your passwords regularly, or when prompted, to minimise your risk should a data breach involving your details occur.

What you share & what you know

The prevalence and growing integration of technology in our everyday lives have naturally resulted in a significant amount of data being captured across various sectors. It is important to consider the information we share with applications and services, as well as the people and networks around us. Below are suggestions to consider for enhancing data-conscious behaviours and prioritising privacy and safety.

Permission tools

The availability and accessibility of permissions will vary across devices and accounts; however, they will primarily include location and GPS permissions, access to microphone and camera capabilities, network access, Bluetooth, and more.

- Disable or limit the sharing of location information across devices and accounts. This will enhance the privacy of your location, including information accessed when logging into accounts. You can access this on the device settings and within application settings, where available.
- Limit access to your photo library and/or camera roll. Your photos may include location information. Turn off this feature.

- Turn off or manage access to permissions to your camera, microphone and other features to minimise the exchange of data.

Friends and Family

Friends and family may use and depend on technology to keep in touch and offer support to one another; together you must have a shared understanding of what you can do to further support your privacy and security.

- Talk to your friends and family about what they can post online about you and encourage them to review the privacy and security settings on their devices, apps, and accounts.
- Don't forget that employers, churches, sports teams, groups, and volunteer organisations with which you are involved may potentially share your personal information online. You may be able to opt out of having any images taken of you posted publicly online.

Where possible, double-check new numbers, emails, social media connections and other activity to ensure accounts have not been impersonated.

-

Connected accounts and family sharing

Many applications are designed to help you stay connected with family and friends, whether by accessing a shared bank account or opting into family sharing. It is important to consider the safety and privacy of all parties involved.

- When opting into a shared account, review the recovery settings.
- Review the opt-out or account closure procedure and what that entails. For example, consider if other individuals will be notified if you delete the application.
- Keep your account credentials (username and password) private, and track who you have shared them with.

Acknowledgement

This handout has been created by Wesnet under licence from the National Network to End Domestic Violence.