Secure your online presence

Share safely and protect your privacy

Be mindful of what you post, as criminals can use social media to perform phishing attacks against you. Privacy settings on social media can change so review these regularly.

What should you do?

Consider what you share online.

Could where you live or where your children go to school be identified from your posts? Personal information can be used to inform social engineering attacks, directed at you or your contacts.

Be cautious when approving connection requests from other accounts.

Be especially wary if they have an unusually low number of posts, pictures or connections.

Avoid sharing sensitive personal information and educate your friends and family who may be sharing too much.

Small pieces of information can be put together by adversaries to form a picture about you for identity theft, or to guess account reset questions or login details.

Use a search engine to look for any publicly visible photos or social media accounts.

If you are not happy with the amount of personal information visible, adjust the privacy settings or delete old social media accounts you no longer use.

Be mindful when signing up to sites using your social logins such as Google, Facebook or Twitter.

If breached, attackers can gain access to all services authenticated via your social account.

Use strong unique passphrases for separate accounts and enable multi-factor authentication where possible.

Only verify account requests or login attempts if you made the request.

For more tips on risks within social media and apps, visit: https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/user-education/security-tips-social-media-and-messaging-apps

Cyber Security NSW