TOP TEN PRIVACY TIPS

1. Hackers use phishing emails to access your secure information. Be cautious about all communications you receive and if you think the email is suspicious do not click on any links or open any attachments.

2. Improve your security online by setting up two-factor authorisation. Adding one more step of authenticating your identity makes it harder for an attacker to access your data.

3. Do not always enable geolocation. It's common for websites to ask for you to share your location. In doing so, they build a profile around your location and interests. Manually select your location instead to better protect your data.

4. Install ad blockers – ads may be tracking you in the background. Use ad blockers to disable tracking and analytics from second and third parties.

5. Be wary of public Wi-Fi networks – these are often less secure than regular networks and give access to more data than necessary when providing Internet connection.

6. You have a right to ask why any information is being collected about you. This includes, for example, state government agencies and other organisations. Their privacy policy may contain this information.

7. Keep your documents and files secure if they contain sensitive or personal information. Consider using encryption to lock portable hard drives and USBs to prevent unauthorised access if they are misplaced.

8. Keep passwords, PINs and other access codes confidential and secure. Using a password manager is a good way of keeping your passwords and logins secure as they are stored in encrypted databases.

9. Enable privacy settings and review them regularly when using online social media and networking sites (e.g. Facebook, Twitter). Consider making your social media profiles private.

10. Securely dispose of mail that contains personal details (e.g. shredding). Never put sensitive documents that have your personal details in the recycle bin.

ipc Information and Privacy Commission NSW
www.ipc.nsw.gov.au
@IPCNSW
/company/information-and-privacy-commission-nsw