Cyber security guide on a page

Each of us have an important role to play in protecting the confidentiality, integrity and availability of NSW Government data and systems. This guide provides security advice to inform and support you in mitigating key cyber security threats, including:

Social engineering attacks, which aim to manipulate people to provide confidential or personal information that can be used for fraudulent purposes.

Identity theft, which is when personal information is accessed and used without consent.

Ransomware attacks, which use malicious software that makes data or systems unusable until the victim pays a ransom.

Secure your accounts

- **Beware of suspicious emails, texts and phone calls:** Stop and think before clicking on links or sharing personal information. Never give out credit card details, bank account details or passwords.
- **Use long, complex and unique passwords:** Adversaries can crack short passwords with little time or effort. Create long passphrases by combining four or more unrelated words (e.g. CircleBitGreySpark*7).
- **Enable multi-factor authentication (MFA):** With MFA enabled, even if an attacker has your password, they will not be able to progress further without that second factor of authentication.

Secure your remote working

- **Use a personal mobile hotspot (not public wi-fi):** Public wi-fi is insecure and can expose your internet activity to monitoring by cybercriminals. Set up a personal mobile hotspot rather than using public wi-fi.
- **Enable encryption and be careful with your devices:** Know where your devices are at all times when working remotely and enable encryption if your device supports it.
- **Plan ahead:** If for any circumstances you are required to work from overseas, engage your IT team early. Have your ICT contact details readily available in case of compromise, loss or theft.

Secure your devices

- **Manage multiple devices securely:** Use work accounts for work only. Avoid sharing your work devices with others and signing into your accounts on someone else's device.
- **Lock your devices:** If you are stepping away from your desk, lock your screen with a unique passphrase or biometrics.
- **Restrict the sensitive information apps can access:** Only use reputable and trusted software and apps, and consider restricting permissions to your contacts, location and other information.
- **Enable automatic updates:** Cybercriminals actively scan the internet for devices that are running vulnerable software versions. Enable automatic updates for all digital devices.
- **Back up your important files:** Back up data to the cloud or another secure and known external storage device. Never plug in unknown external drives you find into your device.

If you think you have been a victim of identity theft, reach out to:

ID Support NSW
1800 001 040
idsupport@customerservice.nsw.gov.au

For more information contact:

Cyber Security NSW
info@cyber.nsw.gov.au

Secure your social media

- **Check your privacy settings and what is publicly visible:** Be mindful of what you share online – could where you live or where your children go to school be identified from your public posts.
- **Keep your social media accounts secure:** Use strong unique passphrases for separate accounts and enable MFA where possible. Only verify account requests or login attempts if you made the request.

Secure your communication

- **Spot a phish and report it:** Know the tell tale signs of phishing emails and report them immediately to your IT Security team. These signs include: lack of context, unusual URLs, unknown senders, poor grammar, and seeking to bypass the usual business process.
- **Secure your video calls:** Only share meeting invitations via private channels, join meetings from private locations and unplug/cover webcams when not in use.