Department of Customer Service

Cyber security guide

For NSW Government staff

NSW GOVERNMENT

Overview

Cyber Security NSW leads, implements and supports cyber security initiatives to achieve the vision of a cyber-secure NSW Government. To assist departments, agencies and local councils, Cyber Security NSW delivers a wide range of products, services and best practice advice and guidance.

NSW Cyber Security Policy

The NSW Government is currently leading the nation by requiring its entities to assess and report on their cyber security maturity. In 2019, the NSW Government released the first iteration of the NSW Cyber Security Policy.

The policy outlines the mandatory requirements all agencies must comply with to ensure cyber security risks to their information and systems are appropriately managed.

The NSW Cyber Security Policy is not mandatory for state-owned corporations, local councils or universities; however, its implementation is recommended as a foundation of strong cyber security practice.

Visit
https://www.digital.nsw.gov.au/policy/cyber-security
for more information

Your role as a member of the NSW public service

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 that aim to manipulate people to provide confidential or personal information, which can be used for fraudulent purposes. There are many forms, the most common being phishing.

Identity theft

when personal information – such as driver licences, passports and bank details – is accessed and used without consent. This information may be used to steal money or commit fraud.

Ransomware

attacks that use malicious software to make data or systems unusable until the victim pays a ransom. It is NSW Government policy never to pay a ransom, as it can encourage further cyber attacks.

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 information such as credit card details, bank account details or passwords. Consider the following to help you identify what may be a phishing attempt:

- Is the message urgent, threatening or offering a reward?
- Does the email address or phone number appear legitimate?
- Is the message asking you to click on a link or provide sensitive information?

It may be difficult to recognise what is real and what is not. Adversaries can use publicly available information about you to add a personal touch that makes it more convincing.

If you receive suspicious correspondence at work, do not interact with it. Instead, report the message to your IT security team.

Use long, complex and unique passwords

Adversaries can crack a shorter password with little time or effort, so make your password longer to be stronger. Create a long passphrase by combining four or more unrelated words (e.g. CircleSeagullBrownSparkle$9).

- Use a different password for each account. This limits access to your other accounts if a password is breached.
- Check if any of your email accounts have been exposed in a data breach and change all passwords associated with any breached accounts: https://haveibeenpwned.com
- Do not use a password that is easy to guess (e.g. birthdays or pets' names) and set strong security questions as threat actors can obtain information about you from online sources.
- Where possible, use a reputable password manager with a long, unique master passphrase. The master passphrase is a gateway to all your accounts, so make sure it is strong and memorable.

Enable multi-factor authentication (MFA)

MFA makes it significantly harder for someone to gain unauthorised access to your accounts. With MFA enabled, even if an attacker has your password, they will not be able to progress further without that second factor of authentication.

- For example, choose to get a code sent to another device when logging in online. This is an added layer of security on your accounts. Other types of MFA include biometrics such as a fingerprint or facial recognition.

For more information on passphrases and MFA, visit **https://www.cyber.gov.au/protect-yourself/securing-your-accounts/passphrases**

Secure your devices

01

Manage devices securely

In the course of your employment you may have been issued multiple digital devices to perform your duties. Ensure you manage these devices securely.

- Avoid sharing your work devices with others to reduce the risk of sensitive information being inappropriately accessed.
- Avoid signing into your accounts on someone else's device to reduce the risk of sensitive information being synchronised to their device.
- Use your work account for work purposes only, and your personal accounts for personal use only. Ensure you use different, unrelated passwords between both accounts.

02

Consider the sensitive information your applications can access

Software and applications can ask for permission to access information, such as your location, contacts, camera, files and microphone.

- Consider restricting these permissions in your privacy settings, even for well-known software and applications.
- Only use reputable software and applications downloaded from trusted app stores and websites.
- Regularly assess the applications on your devices and delete the ones you no longer use.

03

Lock your devices and never leave them unattended

Never leave your devices unattended. If you are stepping away from your device, lock your screen with a unique passphrase or biometric, such as facial identification or fingerprint scanning.

04

Enable automatic software updates

Cybercriminals actively scan the internet for devices that are running vulnerable software versions. Enable automatic updates for all digital devices – including smart TVs, smart watches and anything connected to the internet – to benefit from the latest security features.

05

Back up important files

Protect your important information by regularly backing it up.

Backing up your files helps you recover your information if it is ever lost, stolen, compromised by malicious software or damaged.

- Back up data to the cloud or another secure and known external storage device.
- Only use storage devices from reputable sources. If you find a USB or external hard drive lying around, never plug it into your device, as it could contain hidden malware.

Secure your social media

Check your privacy settings and what is publicly visible

Be mindful of what you post as criminals can use social media to perform phishing attacks against government staff. Review your privacy settings regularly, as these often fluctuate.

Keep your social media accounts secure

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, especially 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 old 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 that social account.

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 video calls

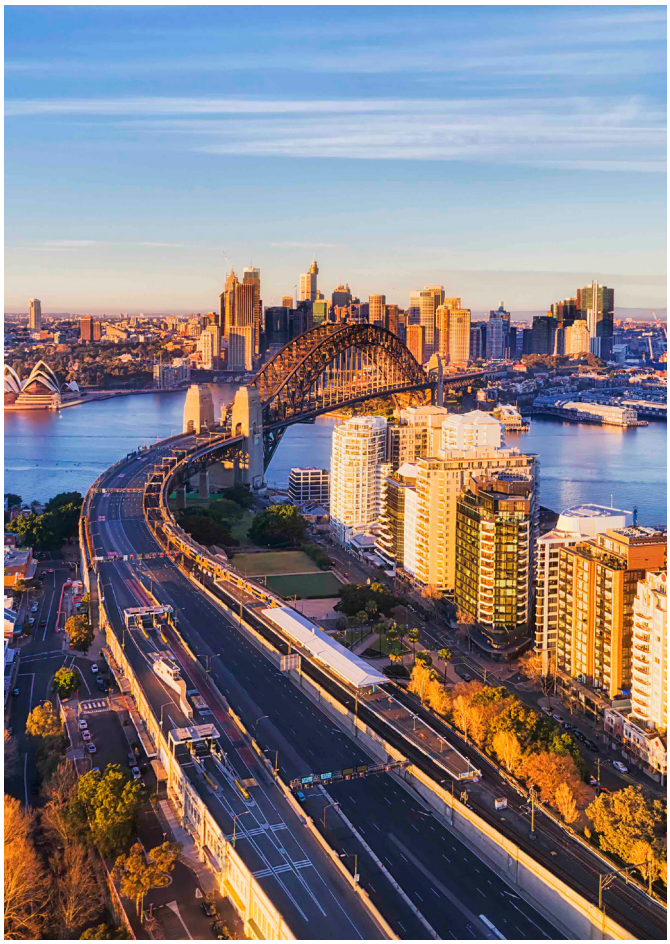
Point your webcam away from any sensitive information in your background and always unplug or cover webcams when not in use.

Be careful when sharing your screen. It is best practice to only share specific software or applications instead of your entire screen.

Secure your remote working

Never use public wi-fi for work devices

Public wi-fi is insecure and can expose your internet activity to monitoring by cybercriminals. When you are travelling, set up a personal mobile hotspot rather than using public wi-fi. Disable wi-fi, Bluetooth, GPS, near field communications (NFC), cellular and any other connectivity functions.



Avoid leaving devices unattended

One of the biggest risks to your information is from lost or stolen devices. Know where your devices are at all times when working outside of the office, and enable encryption if your device supports it.

- Develop the habit of using keyboard shortcuts to lock screens whenever you step away from your device, even for a moment.
- Use the 'find my device' function, or the ability to remotely erase your information to provide additional security in the event of loss or theft.

Secure your home wi-fi

Secure your home internet by changing your default home wi-fi password to a strong passphrase and enabling the guest wi-fi feature for visitors. For a step-by-step guide, see the Guide to Securing Your Home Wi-Fi: https://www.digital.nsw.gov.au/policy/cyber-security/cyber-security-resources/cyber-security-awareness-resources

Speak to your IT team early if you need to travel for work and have their hard copy contact details ready in case your device is compromised, lost or stolen

For information on travelling securely, see the below circular:

DCS-2022-03 Accessing NSW Government digital systems while overseas

Department of Customer Service

Contact details:
If you think you have been a victim of a cyber attack, your first point of contact should be your organisation's IT Service Desk. Keep their details handy in case you lose access to your devices.

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

NSW GOVERNMENT