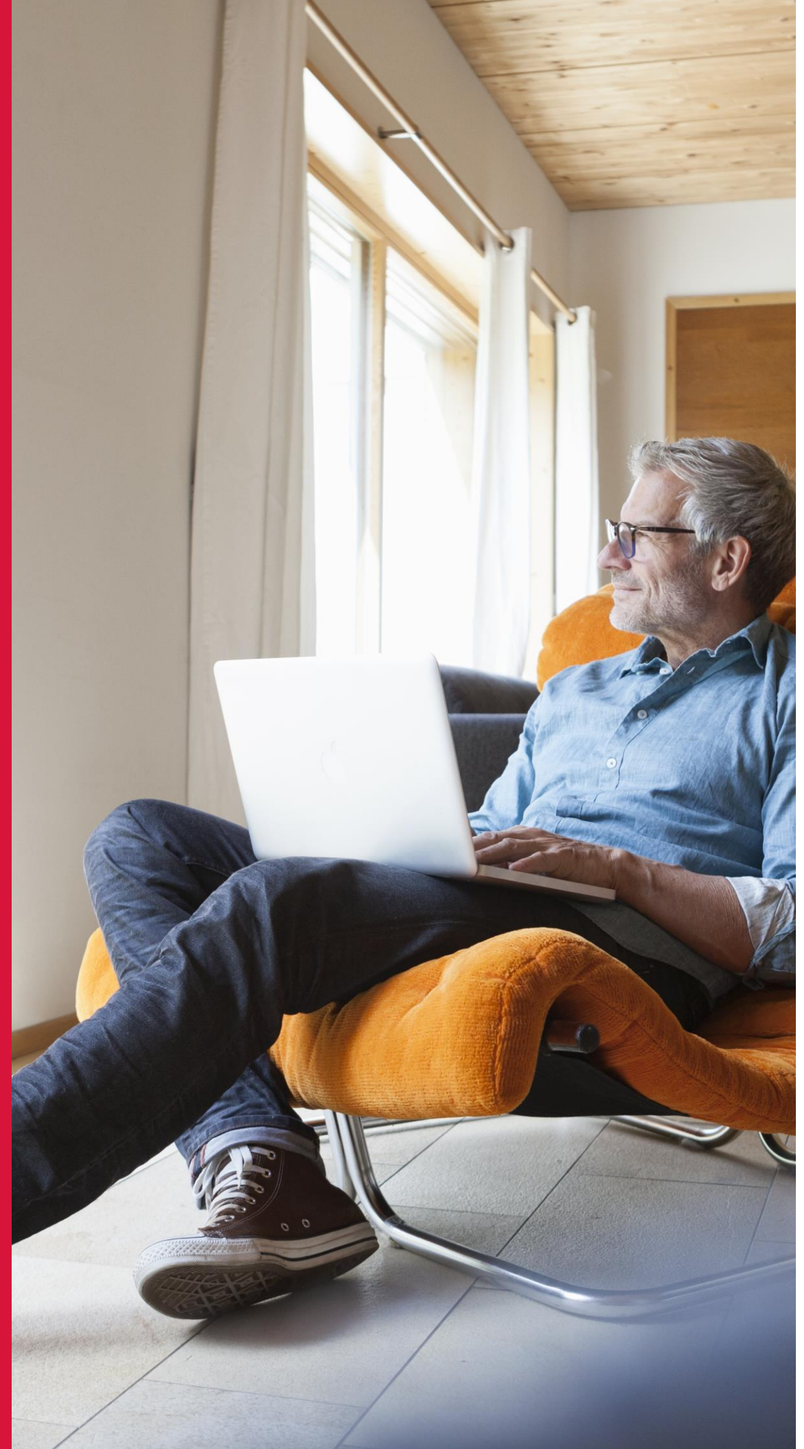
Cyber hygiene tips

Cyber Security NSW

A cyber safe NSW: connected, protected & trusted.



NSW GOVERNMENT

Contents

01

CYBER TIPS

Why your cyber security is essential

01 Almost 70%[1] of successful cyber attacks succeed due to a human element

02 Phishing is the most common point of entry for successful cyber attacks

[1] Source: Verizon Data Breach Investigations Report 2024

TIPS FOR DETECTING PHISHING EMAILS

Is the email **urgent, rewarding** or **threatening**?

Are there **grammatical errors** or **spelling mistakes**?

Does the email address **appear legitimate**?

Does it ask you to change your password or for **sensitive information**?

Do the **links look suspicious** if you **hover** over them?

If you identify a phishing email and haven't clicked on any links or attachments:

- Report the email to your IT Security team
- Delete the email

If you have clicked on a link, opened an attachment or provided your personal information:

- Report the email to your IT Security team immediately
- Follow the steps provided to you by IT Security
- Change your password
- Contact ID Support if you require identity theft advice and support

CYBER HYGIENE CHECKLIST: AT WORK

1. Keep your **passwords/passphrases** secure

- ☐ I use **unique** passwords for each of my accounts
- ☐ I don't write my passwords down and **don't share** them
- ☐ I use **passphrases** that are 14 characters or longer, according to **my organisations policy**.
- ☐ I use **unpredictable** combinations of words for passphrases
- ☐ I use a reputable **password manager** where available
- ☐ I enable **multi-factor authentication** where available

2. **Lock your devices** when you walk away

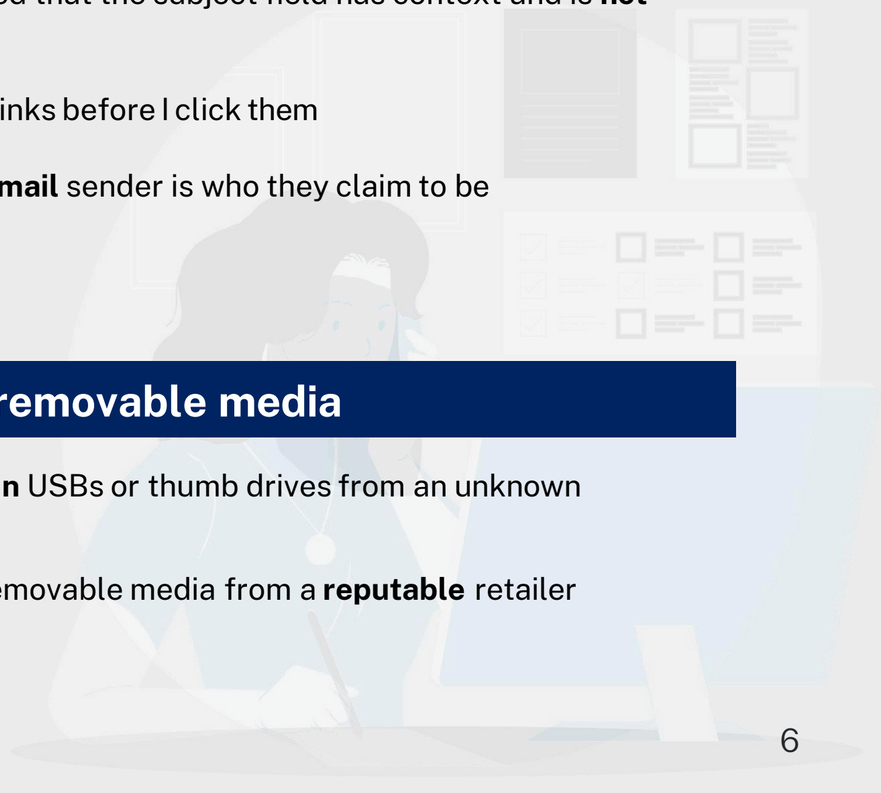
- ☐ I **lock** my laptop, tablets and mobile devices when I am away, even for a short period
- ☐ I know how to use the windows+L key **shortcut** to lock my device (or command+control+Q or Touch ID on mac)

3. Spot and report **phishing**

- ☐ I am aware of my agency's cyber **reporting procedures**
- ☐ I have scanned the email for spelling or **grammatical errors**
- ☐ I have checked that the subject field has context and is **not generic**
- ☐ I **hover** over links before I click them
- ☐ I **verify the email** sender is who they claim to be

4. Use trusted **removable media**

- ☐ I **never plug in** USBs or thumb drives from an unknown source
- ☐ I purchase removable media from a **reputable** retailer



CYBER HYGIENE CHECKLIST: AT WORK

5. Keep **work emails** for work

- ☐ I only use my personal email for **non work-related** activities
- ☐ I use **different passwords/passphrases** for work accounts and personal accounts

6. Connect to **trusted** and **secure Wi-Fi** networks

- ☐ I **never** connect to **public Wi-Fi** using my corporate device
- ☐ I have secured my **home Wi-Fi** when working from home using the guide available here: https://www.digital.nsw.gov.au/delivery/cyber-security/resources/cyber-security-awareness-resources

7. Have a **back-up** plan

- ☐ I work on files that are backed up as my agency recommends as best practice for storing data, i.e. through OneDrive, SharePoint, etc.

For more information and resources, visit our website here:
https://www.digital.nsw.gov.au/delivery/cyber-security/resources

CYBER HYGIENE CHECKLIST: AT HOME

1. Keep your **passwords/passphrases** secure

- ☐ I use **unique** passwords for each of my accounts
- ☐ I don't write my passwords down and **don't share** them
- ☐ I use **unpredictable** combinations of words for **passphrases**, totalling around 20 characters long
- ☐ I use a reputable **password manager**
- ☐ I use **multi-factor authentication** wherever it is available
- ☐ I have **checked** https://haveibeenpwned.com for my breached accounts and changed these passwords

2. Enable **automatic** software and device **updates**

- ☐ I make sure I **apply updates** to all my devices including smart technology I use such as smart TVs, internet connected light globes, and other **Internet of Things** (IoT) devices.
- ☐ I have reviewed the **latest advice** on software updates provided by the Australian Cyber Security Centre https://www.cyber.gov.au/learn-basics/explore-basics/update-your-devices

3. Spot and report **phishing**

- ☐ I have reviewed awareness materials on **phishing indicators**
- ☐ I **hover** over links before I click them
- ☐ I **verify the email** sender is who they claim to be
- ☐ I follow Cyber Security NSW's tips on best ways to **spot phishing** scams

4. **Back-up** your devices regularly

- ☐ I am backing up my devices to the **cloud** and/or an **external drive**

5. Use trusted **removable media** and **cover webcams**

- ☐ I **cover or unplug** my **webcam** when I'm not using it
- ☐ I **turn off** or **unplug** my **microphone** when I'm not using it
- ☐ I only plug in removable media and devices that I have purchased from **reputable** retailers (USB's, CD's, external drives, SD cards, etc.)

CYBER HYGIENE CHECKLIST: AT HOME

6. Confirm your **antivirus** software is up to date

- ☐ I have purchased my antivirus software from a **reputable** source
- ☐ I have the most **current version** installed

7. Secure your **home Wi-Fi**

- ☐ I have changed the **default password** on my router
- ☐ I have secured my **home Wi-Fi** using the guide available here: https://www.digital.nsw.gov.au/delivery/cyber-security/resources/cyber-security-awareness-resources

8. **Encrypt** your devices

- ☐ I use full disk **encryption** such as **BitLocker** to protect my **Windows** devices. I can visit the Microsoft support website for a detailed guide on checking if my device encryption is active at https://support.microsoft.com/en-us/windows/device-encryption-in-windows-cf7e2b6f-3e70-4882-9532-18633605b7df
- ☐ I use **FileVault** to protect my **macOS** devices. I can visit the Apple support website for a detailed guide on checking if my device encryption is active at https://support.apple.com/en-au/guide/mac-help/mh11785/mac

For more information and resources, visit our website here:
https://www.digital.nsw.gov.au/delivery/cyber-security/resources

02

RESOURCES

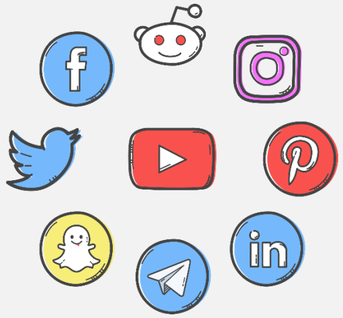
PROTECT YOUR IDENTITY

Prevent and monitor misuse of identity and credentials:

Register for credit check notifications

- For anyone affected by a data breach or wanting to keep their credit score secure.
- Request a temporary ban to ensure no unauthorised credit applications are approved.

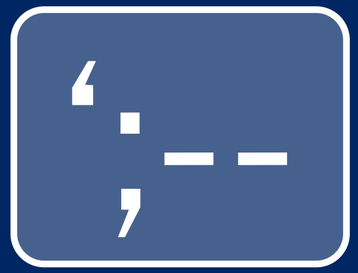
For more information on credit reports and credit scores, visit: https://moneysmart.gov.au/managing-debt/credit-scores-and-credit-reports



Social Media Platforms

- Regularly review privacy settings
- Be mindful of what you post.
- Look up your name on Google and review the level of information available about you.

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

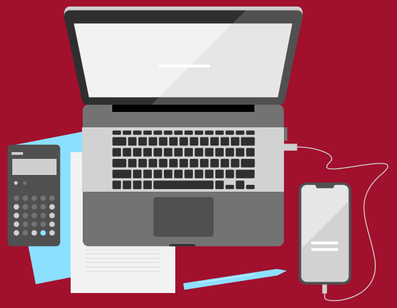


Have i been pwned?

- Check if any of your email addresses have been part of a data breach.

https://haveibeenpwned.com

For more advice on keeping your identity safe, visit https://www.nsw.gov.au/id-support-nsw/get-support



Secure disposal of digital devices

- Backup your data and factory reset old devices not in use.
- Remove sim and SD cards before disposal.

For more advice on secure disposal of digital devices, see https://www.cyber.gov.au/protect-yourself/securing-your-devices/how-secure-your-device/how-dispose-your-device-securely

GOVERNMENT CYBER SUPPORT

Who	About	Contact
NSW GOVERNMENT	For Information Security related incident reporting or advice, your first point of contact should always be your Agency's CISO.	Please consult your agency's directory or contact your IT Service Desk
	ID Support provides identity theft advice and support, including how to restore the security of your identity if your government proof of identity credentials are stolen or fraudulently obtained.	https://www.nsw.gov.au/id-support-nsw 1800 001 040
ASD AUSTRALIAN SIGNALS DIRECTORATE ACSC Australian Cyber Security Centre	Leads the Australian Government's efforts to improve cyber security. ASD works with our business, government and Academic partners and experts in Australia and overseas to investigate and develop solutions to cyber security threats.	https://www.cyber.gov.au/report-and-recover/report 1300 CYBER1 (1300 292 371)
eSafety Commissioner	Leads and coordinates the online safety efforts of government, industry and the not-for-profit community in Australia. eSafety helps safeguard Australians at risk from online harms and promote safer, more positive online experiences.	https://www.esafety.gov.au/
ScamWatch Stop. Better safe than scammed.	Leads the Australian Government's efforts to improve cyber security. ASD works with our business, government and Academic partners and experts in Australia and overseas to investigate and develop solutions to cyber security threats.	https://www.scamwatch.gov.au/report-a-scam