1. Introduction

1.1 What is personal cyber security?

In an increasingly tech-driven world we use devices and accounts every day that are vulnerable to cyber threats.

- Your devices may include computers, mobile phones, tablets and other internet connected devices.
- You also may use online accounts for email, banking, shopping, social media, gaming and more.

Personal cyber security is the continuing steps you can take to protect your accounts and devices from cyber threats.

1.2 What are cyber threats?

The main cyber threats affecting everyday are scams and malware.

- **Malware is a blanket term used to describe malicious software designed to cause harm.** This can include viruses, worms, spyware, trojans and ransomware. Cybercriminals use malware to steal your information and money, and control your devices and accounts.
- **Scams are messages sent by cybercriminals** designed to manipulate you into giving up sensitive information, or to activate malware on your device.

These attacks can have significant personal and financial impact on victims. They are also growing in sophistication and frequency.

1.3 How can this guide help protect me from cyber threats?

If you are learning about cyber security for the first time, or are keeping yourself up to date, this guide is an excellent place to start.

2. Turn on automatic updates

2.1 What are updates?

An update is an improved version of software (programs, apps and operating systems) you have installed on your computer and mobile devices.

- **Software updates help protect your devices** by fixing software ‘bugs’ (coding errors or vulnerabilities). Cybercriminals and malware can use these ‘bugs’ to access your device and steal your personal data, accounts, financial information and identity.

- **New software “bugs” are constantly being found** and exploited by cybercriminals. Updating the software on your devices helps protect you from cyber-attacks.

2.2 How do I set up automatic updates?

Automatic updates are a default or "set and forget" setting that installs new updates as soon as they are available.

- **Turn on and confirm automatic updates** on all software and devices.
- **How you turn on automatic updates can differ** depending on the software and the device.
- **Set a convenient time for automatic updates** if possible, such as when you're asleep or not typically using your device.

2.3 Your device must be powered on, plugged into power and have unused storage space.

Tip. If you receive a prompt to update your device's software you should do so as soon as possible.

2.4 What if the automatic update setting is unavailable?

If the automatic update setting is unavailable, you should regularly check for and install new updates through your software or device's settings menu.

2.5 What if my older device and software do not receive any updates?

If your device, operating system or software is too old, it may no longer be supported by the manufacturer or developer.

When products reach this "end of support" stage they will no longer receive updates. This can leave you vulnerable to cyber-attacks. Examples of products that are end of support include Windows 7 operating system and the iPhone 6.

If your device, operating system or software has reached end of support, we recommend upgrading as soon as possible to stay secure.

3. Activate multi-factor authentication (MFA)

3.1 What is MFA?

You can use multi-factor authentication (MFA) to improve the security of your most important accounts. MFA requires you to produce a combination of two or more authentication types before granting access to an account.

- **Something you know** (e.g. a PIN, password or passphrase).
- **Something you have** (e.g. a smartcard, physical token, authenticator app, SMS or email).
- **Something you are** (e.g. a fingerprint, facial recognition or iris scan).

MFA makes it harder for cybercriminals to gain initial access to your account. It adds more authentication layers, requiring extra time, effort and resources to break.

Tip. Two-factor authentication (2FA) is the most common type of MFA, requiring two different authentication types.

3.2 Why should I activate MFA on all of my accounts?

Using MFA on your accounts makes them much harder for cybercriminals to access. Cybercriminals might manage to steal one authentication type (such as your password), but they still need to obtain and use the other MFA method/s to successfully access your account, requiring extra time, effort and resources.

3.3 How can I activate MFA to protect my most important accounts?

The steps for activating MFA are different depending on the account, device or software application. You should activate MFA now, starting with your important accounts:

- All online banking and financial accounts (e.g. your bank, PayPal).
- All email accounts (e.g. Gmail, Outlook, Hotmail, Yahoo!).
- Accounts that save or use your payment details (e.g. eBay, Amazon, PayPal).
- All social media accounts (e.g. Facebook, Twitter, WhatsApp).
- Any other accounts that hold personal information (e.g. myGov, Apple ID, iCloud, Uber).

3.4 How can I increase my MFA security?

While all forms of MFA provide significant advantages over single-factor authentication (e.g. only a passphrase, password or PIN), some methods are more effective.

MFA is most effective when the method you use is “something you physically have”, such as security keys. You may use smartcards as MFA at work, another highly effective MFA method.

Physical tokens and authenticator apps that generate a one-time PIN or code are also effective MFA methods. Ensure you never share these codes with anyone, and beware of scam messages (phishing) that attempt to trick you into sharing these codes.

3.5 What are the most effective MFA methods for home users?

- **Security Keys**: a small physical security key which may use a physical button, Bluetooth, Near Field Communication (NFC) and/or USB to authenticate the user.
- **Physical Tokens**: a small physical device that generates a one-time PIN (usually six digits) only usable for a short period of time.
- **Authenticator Apps:** an app on your smartphone or tablet that generates a one-time PIN only usable for a short period of time.

3.6 How can I implement the more effective MFA methods on my accounts?

If your account uses less effective MFA methods, such as email or SMS, you should change to a more effective method such as a security key, physical token, or authenticator app. When creating new accounts, activate the most effective MFA methods.

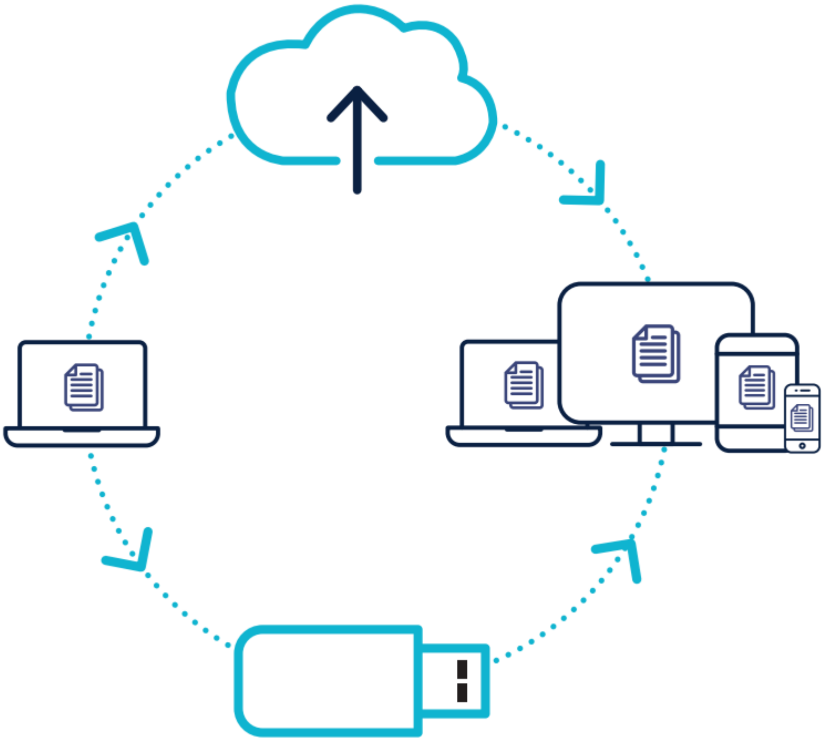
Tip. Prioritise changing to more effective methods of MFA on your most important accounts first. These include banking, email, social media, and accounts with access to financial or personal information.

4. Regularly back up your devices

4.1 What is a backup?

A backup is a digital copy of your information. This can include things like photos, financial information or records that you have saved to an external storage device, or to the cloud.

Backing up your information is a precautionary measure so that it can be recovered if it is ever lost, stolen or damaged.



4.2 How do I back up my devices and files?

You should regularly back up your files and devices. What that looks like, whether it is daily, weekly or monthly, is ultimately up to you. How many times you backup could depend on the number of:

- New files you load onto your device
- Changes you make to files

Tip. Check your backups regularly so that you are familiar with the recovery process. Always make sure your backups are working properly.

5. Use passphrases to secure your important accounts

Multi-factor authentication (MFA) is one of the most effective ways to protect your accounts from cybercriminals. **If MFA is not available**, a unique strong passphrase can better protect your account compared to a simple password.

5.1 What is a passphrase?

A passphrase uses four or more random words as your password. For example: “crystal onion clay pretzel”.

- **Passphrases are more secure** than simple passwords.
- Passphrases are **hard for cybercriminals** to crack, but **easy for you** to remember.

5.2 How can I create a passphrase?

Create passphrases that are:

- **Long:** at least 14 characters long, using four or more random words. The longer your passphrase the more secure it is.
- **Unpredictable:** use a random mix of four or more unrelated words. No famous phrases, quotes or lyrics.
- **Unique:** not re-used across multiple accounts.

If a website or service requires a complex password including symbols, capital letters, or numbers, you can include these in your passphrase. Your passphrase should still be long, unpredictable and unique for the best security.

Password1
crystal
onion clay
pretzel

5.3 Which accounts should I secure with a passphrase?

If your most important accounts are not protected with MFA, change your passwords to unique strong passphrases, starting with:

- Online banking and financial accounts
- Email accounts

If you have a lot of email accounts, prioritise those that are linked to your online banking or other important services. You can typically change your password to a unique strong passphrase through your account settings menu.

5.4 How can I protect my accounts with unique and strong passphrases?

Tip. If you have a lot of accounts to secure, prioritise the following:

- Accounts that save or use your payment details.
- User accounts on your personal devices.
- Social media accounts.
- Any other accounts that hold personal information.
- Accounts who have had their details leaked online (see the following steps).

Tip: Always remember to never reuse a passphrase across multiple accounts.

5.5 How can I check if my account details have been leaked online?

To check if any of your account usernames and passwords have been leaked online by cybercriminals, take the following steps:

1. Visit the Have I Been Pwned website to see if account details tied to your email address/es have been leaked online in a data breach for anyone to see.
2. If this search returns any results, immediately change your password or passphrase for those accounts and enable MFA if possible.
3. Make sure you haven't used the breached password or passphrase on any other accounts, if you have, change these too and enable MFA if possible.

Ensuring your accounts have unique passphrases is vital, as reusing a passphrase allows cybercriminals to easily take control of all of your accounts that use the same passphrase if it is leaked online.

6. Use a password manager to remember your passphrases

A password manager is a tool which helps you securely store and manage strong passwords and passphrases. Its two main functions are the secure storage of your existing passphrases, and assistance with generating new secure (randomly generated) passwords. Password managers are available on computers and mobile devices. Ensure that any password manager you use comes from a trusted and reputable source.

6.1 How can I remember the unique passphrases I've set for my accounts?

Having trouble remembering each unique passphrase you use to secure your accounts? Many people use a password manager which can securely store your passphrases.

6.2 What steps can I take to secure all my accounts using a password manager?

1. **Activate MFA for your password manager to add an additional layer of security.** Using MFA for your password manager means that even if a cybercriminal gains access to its master password, they wouldn't be able to access the data without access to the accompanying MFA code or token.

2. **Ensure that your password managers' master password is your strongest password.** Use a unique strong passphrase as your master password.
3. **Generate long and secure passwords using your password manager.** Use your password manager to generate strong and long randomised passwords to further secure your accounts. Password managers can quickly generate passwords tailored to your criteria (e.g. you could create 50 character passwords with upper and lowercase letters, numbers, and special characters for every account).
4. **Add accounts to your password manager.** Every time you login to an existing account that is not in your password manager, change the password into a strong randomly generated password and store it using your password manager.
5. **Use your password manager to fill in the password fields when logging in for you.** For ease of use, password managers typically have browser extensions (always check for authenticity before installing these) to auto-fill login pages with your saved username and password, and the option to copy-paste your credentials into login fields. This can be used to streamline logging into accounts with long secure passwords (e.g. a randomly generated 50-character complex password).

Tip. Every time you login to an account, add your login details (username and passphrase) to your password manager and, if needed, change any old insecure passwords into unique strong passphrases.

7. Secure your mobile device

Today smartphones and tablets are used in everyday life. We use them to connect, shop, work, bank, track our fitness and complete hundreds of tasks at any time, and from any location.

7.1 What can happen if my mobile device is compromised, lost or stolen?

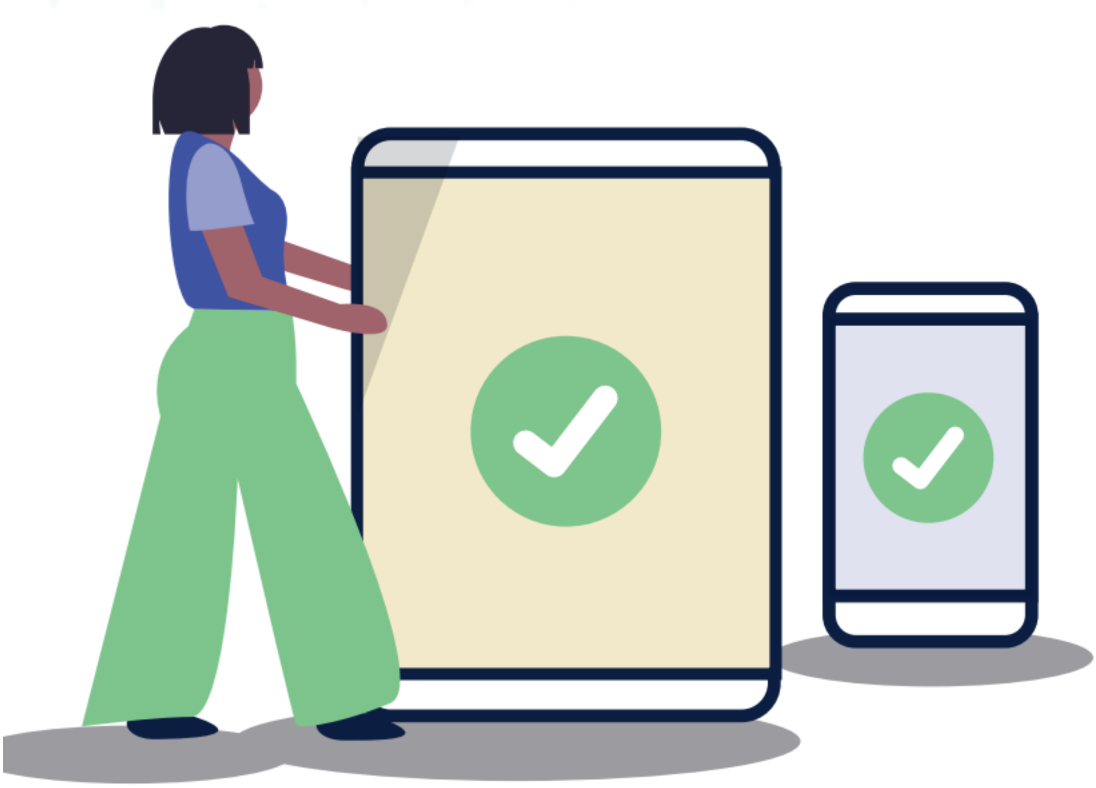
- It may be used by cybercriminals to steal your money or identity. They do this by using information stored on your device, including social media and email accounts.
- You may lose irreplaceable data like photos, notes or messages (if it is not backed up).
- A cybercriminal may use your phone number to scam other people.

7.2 How do I secure my mobile device?

7.2.1 Device Security

- **Lock** your device with a passphrase, password, PIN or passcode. Make it difficult to guess – your date of birth and pattern locks are easy for anyone to guess. Use a passphrase for optimal security. You might also consider using facial recognition or a fingerprint to unlock your device.
- **Ensure** your device is set to automatically lock after a short time of inactivity.
- **Don't** charge your device at a public charging station and avoid chargers from third parties.

Treat your phone like your wallet. Keep it safe and with you at all times.



7.2.2 Software and App Security

- **Use** your device's automatic update feature to install new application and operating system updates as soon as they are available.
- **Set** the device to require a passphrase/ password before applications are installed. Parental controls can also be used for this purpose.

Check the privacy permissions carefully when installing new apps on your device, particularly for free apps. Only install apps from reputable vendors.

7.2.3 Data Security

- **Enable** the remote locking and wiping functions, if your device supports them.
- **Ensure** you thoroughly remove personal data from your device before selling or disposing of it.

7.2.4 Connectivity Security

- **Turn** off Bluetooth and Wi-Fi when you are not using them.
- **Ensure** your device does not automatically connect to new Wi-Fi networks.

8. Improve your Wi-Fi security habits

8.1 What is a Wi-Fi router?

A home Wi-Fi router is a small electronic box that typically combines router and modem functions to create an internet-connected network for the devices in your home. Here we refer to the device simply as a router.

8.2 How can I improve my Wi-Fi security on mobile devices?

Your internet connection is a way for you to interact with the outside world, but it also provides a channel into your device. If your Wi-Fi connection isn't secure someone may use it to steal your personal or financial information for malicious purposes.

- Disable Bluetooth and Wi-Fi when not in use, especially if you're in a public place
- Use cellular data when not connected to your secure home network

8.3 How can I improve my router security?

8.3.1 Change your router's default username and password

Use the information contained in your router's user manual to access your router settings. If you can't find the user manual a quick internet search of your router model should typically provide you with access to a copy. Some routers have a sticker on the device that also provides your router's IP address and default login details.

- **Open a web browser and type into the address bar your router's IP address.** Your router's IP address will typically start with "192.168.#.#" or "10.0.#.#" (where # represents different numbers), check your user manual for the exact IP address.
- **Enter the router's username and password when prompted.** In your user manual you should also be able to find the default username and password which you will need when logging in to your router.

- **Change the password on your device** using the router settings to a unique strong passphrase.
- **Where possible, also change the default administrator username** (typically "admin" or "administrator") to something hard to guess.

Your router's default administrator username and password may be publicly available online, making it easy for cybercriminals to access if you don't change its default username and password.

8.3.2. Change your default Wi-Fi name and password

- **Change your Wi-Fi name** (also known as SSID) from the default set by the router manufacturer to something that doesn't contain identifiable information. You can do this in the router's settings menu.
- **Ensure your Wi-Fi password** provided by your internet service provider or router manufacturer is long and hard to guess. If not, change it to a unique strong passphrase.

In many cases a cybercriminal can use your router's default Wi-Fi network name to easily determine the make and model of the router you are using and use this information to gain access your router.

Also, if your Wi-Fi password is weak it can be trivial for cybercriminals to break.

8.3.3 Use the strongest Wi-Fi encryption

- **You should change your Wi-Fi encryption** protocol used by your router to WPA3 or WPA2 (if WPA3 isn't supported) in the settings menu.

It is possible for anyone within range of your router to intercept your internet activities if your Wi-Fi is unencrypted or using an outdated encryption protocol.

You should use the strongest encryption protocol provided by your router, which is currently WPA3 (introduced in 2018) or WPA2 (if your router or devices don't support WPA3). If your router does not support WPA2 (as a minimum), you should consider replacing it.

8.3.4 Update your router to use the latest firmware

Firmware is the software on your router that determines the functions it can perform. Just like new software updates for your computer, new firmware for your router will provide improved features and security.

- **To find out which version of firmware is installed** on your router log in to the device and check its settings.
- **Then go to the manufacturer's website,** it will tell you if there's a more recent version of firmware for your device and allow you to download it.
- Install the updated firmware. Be careful when you do this because a failed update can render your device unusable and disconnect all your devices from the internet. Make sure you follow the instructions in your device's manual and select the correct firmware upgrade version for your model of router.
- If you don't feel confident to updating your **router firmware,** you could contact a reputable computer technician for assistance. You could also think about replacing your router.

8.4.5 Disable remote management and Universal Plug and Play (UPnP)

- Ensure both remote management and Universal Plug and Play (UPnP) are disabled in your router's settings.

Remote management on your modem or router can allow you to make changes to your internet connection, including passwords, by logging into your device via the internet.

UPnP allows devices on your network to automatically discover and communicate with each other using your Wi-Fi network at home or from another location using remote access, without needing authentication.

Disabling remote management and UPnP can increase your security from remote attackers.

Note. PC and console games with online functionality may report network errors if UPnP is disabled. If this occurs, set up manual port forwarding in your router's settings.

8.4.6 Enable Guest Wi-Fi

- **Consider enabling the "Guest" Wi-Fi feature** in your router's settings.

Visitors can use Guest Wi-Fi for internet access in your home, but won't have your Wi-Fi passphrase/ password or access to your main Wi-Fi network.

8.5 Should I upgrade my old router?

Manufacturers often classify old devices as 'legacy' models and no longer develop firmware upgrades for them, which can leave you exposed to known security vulnerabilities.

Upgrading to a current router model will offer you significant benefits such as additional features and configuration options, the latest encryption, and faster data transfer speeds.

8.6 How can I protect myself when using public Wi-Fi?

Public Wi-Fi "hotspots" like cafes, airports, hotels and libraries are convenient, but they can be risky. It's easy for information sent using public Wi-Fi to be intercepted, so you need to be careful about what information you send or receive while connected.

When using public Wi-Fi follow these suggestions to stay secure:

- Avoid sending or receiving sensitive information while connected to public Wi-Fi networks.
- When online banking or shopping, sending confidential emails, or entering passphrases/passwords or credit card details into websites, switch to your cellular data connection or wait until you're on a secure home or office connection.
- Always try to confirm the 'official' hotspot name from venue staff and manually connect your device to it.
- Do not let your device automatically connect to public Wi-Fi networks by disabling this option in your device's Wi-Fi settings.
- Remember to disconnect from the Wi-Fi network and clear it from your device after you have finished using it.

9. Secure Your Internet Of Things (IoT) Devices

9.1 What is an Internet of Things (IoT) device?

An IoT device is an everyday item that has had internet connectivity added to it. Examples of IoT devices include smart fridges, smart televisions, baby monitors and security cameras. IoT devices within homes and businesses generally use Wi-Fi or cellular networks to connect to the internet.

9.2 Why do I need to secure my IoT devices?

Many IoT devices commonly found in Australian homes and businesses have not been designed with security in mind. If your IoT devices have known unpatched security vulnerabilities, it can allow cybercriminals to access your device, network and personal data for malicious purposes.

9.3 What can I do before purchasing an IoT device?

You should research IoT devices before making a purchase, as manufacturers provide varying levels of security. Things to consider include:

1. **Is the device made by a well-known reputable company and sold by a well-known reputable store?** Well-known reputable companies are more likely to produce devices with security in mind. Well-known reputable stores are more likely to have a stricter supply chain, ensuring the device gets to you as intended by the manufacturer.
2. **Is it possible to change the password?** If the device is shipped with a weak default password, it is important you are able to change it. Weak default passwords are an easy way for cybercriminals to attack a device.
3. **Does the manufacturer provide updates?** It is important that companies offer updates to fix security vulnerabilities as they are discovered.
4. **What data will the device collect and who will the data be shared with?** This information should be readily available on the manufacturer’s website or in their

privacy policy. Also consider the information that is collected by the IoT device's online or mobile app.

5. **Does the device do only what you want it to do?** Extra IoT device capabilities that you don't need or won't use (such as connecting to the internet) can increase the device's vulnerability to attacks and reduce your security.

9.4 How should I set up an IoT device?

Keep in mind a few simple questions while setting up your device, to help you keep your network and data more secure.

1. **Does the device need to be connected to the internet?** If you're not going to use the device's features that require internet connectivity, then you should consider whether it needs to be connected. Devices that are not connected to the internet are much less likely to be compromised.
2. **Is the device in a secure location?** Installing your device in a secure location can reduce the risk of physical compromise.
3. **Do I change the default username and password?** If your device is not equipped with a unique strong passphrase or password, then you need to change it. Default usernames and passwords are collected and posted online, leaving your device vulnerable to cybercriminals.
4. **Is my Wi-Fi network set up securely, and does it have a secure password?** Secure your Wi-Fi network and router to make it harder for attackers to access your device and network.
5. **Add device to your Guest Wi-Fi network.** Consider enabling Guest Wi-Fi on your router and add your device to that network to isolate it from the devices on your main network. Keep in mind that some IoT devices require your mobile devices to also be connected to the same network to communicate.
6. **Are unnecessary features turned off?** If your device has unwanted or unnecessary features (such as cameras or microphones), these should be disabled where possible.

9.5 How can I maintain my IoT devices?

There are some important things to remember once your IoT device is set up and in use. These include:

1. **Reboot your devices regularly.** If the IoT device starts to become slow or inoperable, it may mean that malware is present. Some malware is stored in memory and can be easily removed by a device reboot. If the device continues to be slow or inoperable after a reboot, try a factory reset.
2. **Apply regular updates.** Some devices apply updates automatically. For those that don't, regularly check with the manufacturer and apply updates when they become available. When updates are no longer available for your device, consider upgrading to a newer device as soon as possible to reduce security risks to your network.
3. **Turn off your device when it is not in use.** Leaving unused and unmonitored devices powered on and connected to your network for extended periods can increase the likelihood of your devices being attacked.
4. **Watch for a significant increase in your monthly internet usage or bill.** Significant increases can indicate that your device has been compromised with malware. Performing a factory reset or changing the passphrase/password on your IoT device may remove the malware.

9.6 How can I dispose of an IoT device?

Disposing of a device (by discarding or selling it) may give other people easy access to your personal information tor data. Ways to prevent this include:

1. **Erase all data and personal information.** Erasing your personal information ensures that no one gains access to it after you have disposed of the device. The manufacturer should provide a method for how to erase your data and personal information from both the device and associated applications.
2. **Perform a factory reset of the device.** A factory reset is designed to erase data kept in local storage and reset passphrases/passwords, usernames and settings back to default. Check the device's user manual or the manufacturer's website for information on how to perform a factory reset.
3. **Disassociate the device from mobile phones and other devices.** Make sure you check your other devices and remove any pairing with the device you are disposing of. Remove any permissions granted to the mobile application that are no longer needed.
4. **Remove any removable media (e.g. USB flash drives, memory cards etc.) attached to the device.** Removable media may contain personal data that is not deleted in a factory reset and should be physically removed, physically destroyed and disposed of separately from the device.

10. Encrypt Your Computer's Hard Drive

10.1 Why should I encrypt my computer's hard drive?

Performing a full-disk encryption means the entire contents of your computer's hard drive are encrypted, and can only be accessed with a passphrase or password. Even though your device itself might be password protected using a unique strong passphrase, cybercriminals can still access the hard drive and steal your data if it is not encrypted.

10.2 How can I encrypt my computer's hard drive?

You should take care when encrypting your hard drive – if you lose access to the encryption or recovery keys, you will not be able to use the device and will have to wipe everything and start again.

- Check whether disk encryption is enabled on your devices, and turn it on if it is not. Most modern operating systems have some form of disk encryption built in.

10.3 Desktop or Laptop Computers

- On Apple macOS, disk encryption is known as FileVault, and can be enabled in the Security & Privacy section of the System Preferences. When enabled, your login passphrase/password is used to encrypt the hard drive, and any new files that are created are automatically encrypted as they are saved to your disk.
- On Microsoft Windows 10 disk encryption is less straightforward. There is an included encryption tool called BitLocker that is available to users with all versions except Windows 10 Home. Windows 10 Home has a built-in Device Encryption tool, but it is only available to devices that meet certain hardware specifications. Microsoft's website contains information about both of these tools and how they can be configured.
- If your device does not meet the hardware requirements, there are free and open source third party tools available that will allow you to enjoy the same level of protection as the built-in methods.

10.4 Mobile devices

- Recent versions of Apple iOS or Google Android now also have encryption options available. Encryption of some form has been included in mobile devices from iOS 3.0 and Android 4.0, and most devices will now ship with encryption turned on by default. This uses your normal PIN or screen lock passphrase/ password to protect your data.

11. Securely dispose of your devices

11.1 Why should I take steps to securely dispose of a device?

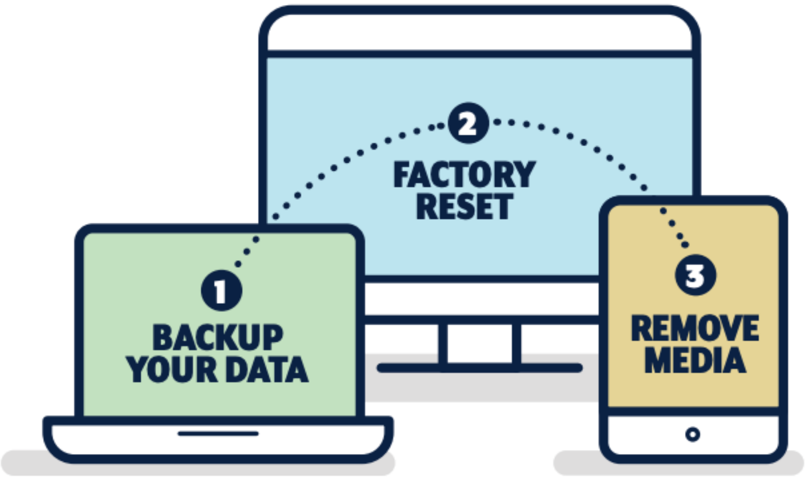
Disposing of a device (by discarding, recycling, selling or giving it away) without taking steps to remove your data may give other people easy access to your personal information and data.

11.2 How can I securely dispose of a device?

Before disposing of your computer, phone, tablet, games console or any other smart device, you should:

1. **Create a backup of your data from the device.** Make sure you have made a backup of any important files and have transferred these to another secure device.
2. **Perform a factory reset of the device and erase all data and information.** A factory reset is designed to erase data kept in local storage and reset usernames, passwords and settings back to default. Erasing your personal information ensures that no-one gains access to it after you have disposed of the device. Check the device's user manual or the manufacturer's website for information on how to perform a factory reset.
3. **Remove any removable media (e.g. SIM cards, SD cards, USB flash drives) attached to the device.** Removable media may contain personal data that is not deleted

in a factory reset and should be physically removed, physically destroyed and disposed of separately from the device.



Remember that disposing of a device without taking steps to remove your data may give other people easy access to your personal information and data.

12. Protect yourself against malware

12.1 What is malware?

Malware is a blanket term for malicious software designed to cause harm, such as ransomware, viruses, spyware and trojans. Malware can:

- Steal your bank or credit card numbers
- Steal your usernames and passwords
- Take control of or spy on your computer

The steps you can take to protect your devices from malware include:

- Enable automatic updates for your devices.
- Be vigilant online: be wary of opening links, emails or files from unknown sources.
- Activate real time protection on your Windows 10 devices

12.2 How do I turn on real time protection to stop malware?

Real time protection is a security feature that helps stop malware from being installed on your device.

This feature is built into Microsoft Defender, a comprehensive antimalware and threat detection program that is part of the Windows 10 security system.

12.3 Why do I need real time protection?

Prevention is better than a cure. Unlike an antimalware scan, which searches for malicious files or programs that are already on your device, real time protection will detect and stop malware before it gets to your device.

How do I activate real time protection?

Real time protection should automatically turn itself on. However, it can be temporarily switched off, so it is important to check that the feature is up and running and is actively protecting your device.

If you are using an anti-malware software, ensure that it is actively protecting you against malware.

13. Turn on ransomware protection

13.1 What is ransomware?

Ransomware is a type of malware that locks down your computer or files until a ransom is paid. It works by locking up or encrypting your files so that you can no longer use or access them. Sometimes it can even stop your devices from working. Ransoms are typically paid using an online digital currency or cryptocurrency such as Bitcoin, which is very difficult to trace.

Note. We recommend you do not pay the ransom as there is no guarantee you will regain access to your information. You may also be targeted by another attack.

Ransomware can infect your devices in the same way as other malware, including:

- Visiting unsafe or suspicious websites.
- Opening links, emails or files from unknown sources.
- Having poor security on your network or devices.

13.2 How can I protect myself from ransomware?

Ransomware protection has the ability to prevent many types of ransomware attacks from happening. In the unfortunate event of an attack, ransomware protection can also interrupt the ransomware from encrypting all your data, which minimises the extent of the damage.

Backups can also assist in recovering your data as part of the recovery process following a ransomware attack.

13.3 How can I activate ransomware protection?

If you are using Windows 10, you can enable built-in ransomware protection to protect your files.

If you are using another operating system, you may need to source and install ransomware protection for your devices.

13.4 How can I backup my devices?

In addition to installing ransomware protection, you should also back-up your information. That way, even if an attack is successful, you will at least have your important information accessible elsewhere.

14. Reduce your digital footprint

14.1 What is my digital footprint?

As soon as you go online, you start creating a trail of information about you. This is known as your digital footprint.

Cybercriminals can use this information against you, by using it to create convincing scams that specifically target you or someone you know.

With a simple Google search, cybercriminals could find your:

- Identifying information (date of birth, middle or maiden name, birthplace).
- Workplace.
- Relationships.
- Hobbies and interests.
- Sporting clubs.
- Educational background.
- Answers to account recovery questions.

Such data could also be used to identify personal details that you have included in your passwords, PINs, or in the answers to your account recovery questions.

This information could be used by cybercriminals to access your accounts and devices.

14.2 How can I reduce my digital footprint?

To reduce your digital footprint:

- Increase your privacy settings on social media sites.
- Consider using an adblocker that can block tracking pixels and social media icons.
- Do not post your personal contact details (such as email address and phone number) online. Remove this information if already posted online.
- Avoid sharing information online that may identify you, or could be answers to your account recovery questions (e.g. your birthplace, or where you went to school). Remove this information if already posted online.
- Delete or deactivate any online accounts that you no longer use.
- Use a search engine to look up your name and review both the image and text results. If you find a result that reveals too much personal information, either take it down yourself or ask the person or company who posted it to delete it.

15. Develop your cyber secure thinking

Personal cyber security is not just about changing settings, it’s also about changing your thinking and behaviours.

15.1 Watch out for cyber scams

Cybercriminals are known to use email, messages, social media or phone calls to try and scam Australians. They might pretend to be an individual or organisation you think you know, or think you should trust. Their messages and calls attempt to trick you into performing specific actions, such as:

- Revealing bank account details, passwords, and credit card numbers
- Giving remote access to your computer
- Opening an attachment, which may contain malware
- Sending money or gift cards

Scam messages can be sent to thousands of people, or target one specific person.

15.2 How do I recognise scam messages?

It can be difficult to recognise scam messages. Cybercriminals often use certain methods to trick you. Their messages might include:

- **Authority:** is the message claiming to be from someone official, such as your bank?
- **Urgency:** are you told there is a problem, or that you have a limited time to respond or pay?
- **Emotion:** does the message make you panic, hopeful or curious?
- **Scarcity:** is the message offering something in short supply, or promising a good deal?
- **Current events:** is the message about a current news story or big event?

Review the guidance about Scams.

15.3 What should I do if I get a scam message?

If you receive a scam message or phone call, you should ignore, delete.

If you've engaged with a scam and think your bank accounts, credit or debit cards may be at risk, contact your financial institution immediately. They may be able to close your account or stop a transaction.

15.4 What if I'm unsure if a message is a scam?

If you think a message or call might truly be from an organisation you trust (such as your bank) find a contact method you can trust. Search for the official website, phone their advertised phone number, or visit a physical store or branch.

Do not use the links or contact details in the message you have been sent or given over the phone as these could be fraudulent.

Tip. Think Before You Click

- Think before you click on links on emails, websites and SMS.
- Always be sceptical of attachments you receive.
- If your browser tells you a website is unsafe, close it immediately.

Remember: No IT person, government department or business will contact you and ask for your login details.

15.5 Take Control Of Your Mailboxes

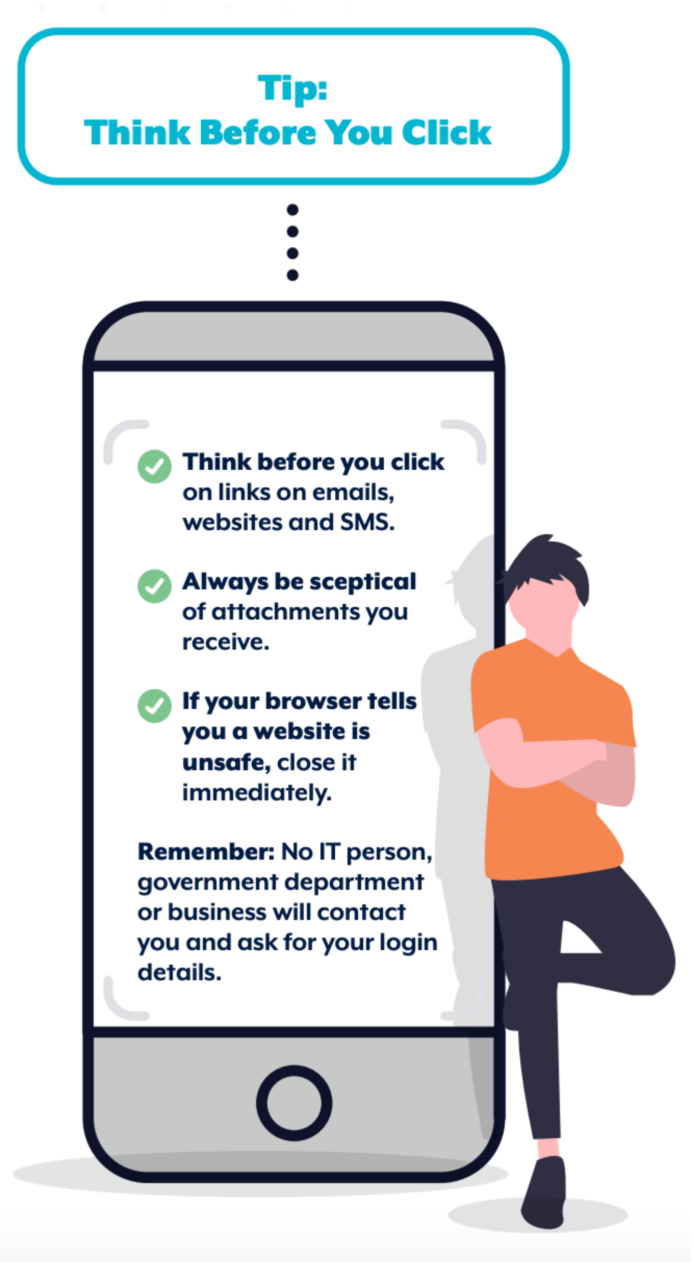
Don’t let your mail accumulate in both your home and email mailboxes. This prevents cybercriminals stealing your emails and physical mail and using it for socially engineered scams or accessing your accounts.

- **Periodically clean out your email inbox** of sensitive personal information and documents (such as copies of IDs, loan and job application documentation). This prevents cybercriminals from stealing this sensitive information if your email account is ever compromised. To do this:
  - **Archive your emails** in a passphrase protected zip-file (and create a backup),
  - **Delete the emails from your account** (and the deleted items/trash folders).
- **Don’t let your mail accumulate** in your mailbox at home.
- **Destroy mail or documents containing personal information** and account details before disposal (e.g. bank statements, bills, and address labels).

15.6 Stop and think before you share on social media

Cybercriminals can use information you have publicly posted on your social media account/s in their scams and cyber-attacks.

Remember information on the internet is permanent and you can never fully remove what has been posted.



✓ **Think before you click** on links on emails, websites and SMS.

✓ **Always be sceptical** of attachments you receive.

✓ **If your browser tells you a website is unsafe,** close it immediately.

Remember: No IT person, government department or business will contact you and ask for your login details.

15.7 How can I stop and think before posting?

- **Think:** How could a cybercriminal use this information to target me or my accounts?
- **Think:** Would I be comfortable showing this information or image to a complete stranger offline?

15.8 What information should I avoid sharing?

Avoid sharing information (including photos) online that cybercriminals can use to identify you, manipulate you through a scam or guess your account recovery questions. This may include your:

- Birthplace and date of birth.
- Address and phone number.
- Employer and work history.
- Where you went to school.
- Any other personal information that can be used to target you.

15.9 Secure Your Apps And Browser Extensions

When using apps and browser extensions on your devices, use the following cyber secure behaviours and thinking:

- **Turn on automatic app updates**, and always update your apps and browser extensions as soon as possible for the latest security protection.
- **Check that your apps and browser extensions are made by reputable publishers** and ask for permissions that are appropriate for their intended use.
- **Uninstall apps and browser extensions** you don’t need or use anymore.
- **Always download apps and browser extensions from an official store** such as Apple’s App Store or Google Play for Android.

16. Security tips for travelling

When travelling, you may be more vulnerable to a cyber attack. Your electronic devices contain personal data and using public networks can be a risk. Cybercriminals will target anyone to steal information or money.

Whether you’re going intercity or overseas, make sure to secure your devices. Especially if you have access to sensitive data on them, such as identity documents or work files.

16.1 Before you travel

Travelling can be a stressful experience. Secure your data, accounts and devices before you leave to help reduce the chance of a compromise.

16.1.1 Safeguard your data

Create a backup of your data that you can keep secure at home. Also, leave behind any information or devices you don’t need. This limits how much data is at risk if someone steals or compromises your devices.

16.1.2 Secure your accounts

Turn on multi-factor authentication (MFA) for your accounts. MFA is when you need 2 or more steps to verify your identity before you can log in. For example, using your login details as well as an authentication code.

Avoid using SMS as an MFA method as it is less secure. Also be aware you need to enable international roaming to get SMS overseas.

Where MFA isn't an option or you need to disable it before travel, use a strong password such as a passphrase. A passphrase is a string of random words like 'crystal clay onion pretzel'. It should be long, unpredictable, unique and should not include personal details.

16.1.3 Secure your devices

Secure your devices with a PIN or passphrase. Make it hard to guess and don't include personal details such as your date of birth. Make sure your devices are set to lock automatically after a short time (less than 5 minutes).

For more security use biometrics if your device supports it, such as your fingerprint. But check the laws of where you are travelling. Some countries may force you to unlock your device if you use biometrics. To avoid this, you can disable biometrics and use a PIN or passphrase instead.

For more protection against unwanted access, encrypt your devices. It means if a device was compromised your data stays secure. If you do encrypt your devices, make sure to back up your recovery keys. If you lose the keys, you won't be able to use your device until you factory reset it or reinstall the operating system.

16.1.4 Keep devices and software up to date

Update any devices you are travelling with so they have the latest security. Check automatic updates are on and install updates as soon as possible. The longer you leave it, the more vulnerable you could be to a cyber attack.

16.1.5 Protect against malware

Confirm you have installed antivirus software and that it is working. Your devices may already have it installed by default.

If you decide to use third-party antivirus software, make sure to research and choose a reputable provider.

16.1.6 Limit what you bring

Consider using a device that is only for travel, such as a burner phone (a cheap phone you can dispose of). This should not have any personal data on it, including accounts or password managers. If someone gains unauthorised access to your device, there is less sensitive data at risk.

16.2 While you travel

Remember to stay vigilant with your security while on your trip with the following tips. This is the period you will be most vulnerable to cyber threats.

16.2.1 Lock and secure your devices

Lock your devices whenever you leave them unattended. Even if it is only for a short period. Make sure your devices are set to automatically lock after a short time (less than 5 minutes).

Try not to leave your devices in your room when you go out, even if there is a hotel safe. When in transit, always keep your devices on you or in sight.

16.2.2 Be wary of public devices

Avoid using public devices such as computers in a hotel business centre. These devices could have malware installed and using them can put your accounts at risk.

If you must use a public device, try not to log into your accounts or input personal information. If you do log in, don't save your login details and remember to log out when done.

16.2.3 Use trusted peripherals

Never use someone else’s peripherals such as chargers, cables and other removable devices. Public charging stations and ports could also put your data at risk. Buy peripherals from reputable stores if you need them.

Avoid using portable storage devices such as USB drives. These are easy to lose, steal or infect with malware. Use more secure methods of file transfer and storage such as cloud services.

16.2.4 Be aware of your surroundings

Avoid accessing sensitive information in public spaces such as airports and hotel lounges. You could expose information to anyone passing by. Wait until you are in a more private location or consider using a privacy screen protector.

16.2.5 Back up your data

Make sure to back up your data often while travelling. If something happens to your device, you can restore important data such as photos and files. Create backups using a secure cloud service or an external storage device. You can turn on automatic backups to reduce the risk.

16.2.6 Limit the information you post

Be careful of sharing your location and personal information on social media. This includes details such as your flight number, hotel check-in or photo metadata. Someone could use this information to target you.

16.2.7 Manage your device connections

Public networks are convenient but can also be unsecure. Cybercriminals will target public networks to gain access to your sensitive information. If you are working in public spaces such as an airport or café, avoid using their Wi-Fi or use a VPN. Before using a VPN, check local laws to make sure it is legal in your current location.

Only use trusted networks such as your mobile data and personal hotspot. Where this isn't an option, think twice about what you share or access on a public network.

Consider turning off Wi-Fi, Bluetooth and near-field communication (NFC) on your devices when not in use. Cybercriminals could use these to hack your device or make unauthorised transactions.

Case study: Identity theft from using public Wi-Fi

A NSW man owed over $7000 in fees to a company for gift cards and subscriptions he didn't buy. The recipients for these purchases went to unknown email addresses. After investigating, he found several inquiries on his credit report. These happened around the same time as the sale of the gift cards and subscriptions. The first inquiry happened not long after he had used his laptop on a trip. When connected to the public airport Wi-Fi, he had sent his ID documents to his parents. These included his passport and birth certificate. Using the airport Wi-Fi may have let cybercriminals access his IDs and steal his identity.

16.2.8 Check for signs of compromise

While travelling you should be alert for signs of compromise, such as:

- Devices or apps keep crashing.
- Suspicious adverts or pop-ups.
- Unexpected activity on your accounts.
- Unknown emails in your sent folder.
- Excessive battery or data usage when using your device.
- Devices are hot to the touch when idle.

16.3 After you travel

When you have returned home, you should still be alert to the possibility of a compromise. To further secure your devices, consider:

- Changing the PINs and passwords for your devices and accounts.
- Disposing of your burner phone if you used one, including any SIM cards, eSIMs or microSD cards.
- Wiping any removable storage used when travelling, such as USB drives or SD cards.

17. Glossary

Account recovery. A process in which a set of questions or other verification methods are used to recover or regain access to an account or to change an account passphrase/password.

App. Also referred to as a mobile application, an app is a term for software that is commonly used for a smartphone or tablet.

Anti-malware. A software program designed to protect a user's computer or network against malware. Also known as antivirus.

Attachment. A file sent with an email message.

Authenticator app. An app used to confirm the identity of a computer user to allow access through multi-factor authentication (MFA).

Backup. A copy of device data stored elsewhere so that it may be used to restore the original.

Browser extensions. An add-on for your internet browser (e.g. Google Chrome, Firefox) that provides additional features, functionality, or appearances.

Cloud. A network of remote servers that provide massive, distributed storage and processing power.

Cellular data connection. The internet connection provided by a SIM card, such as 4G or 5G.

Cellular network. The internet connection provided by a SIM card, such as 4G or 5G.

Cryptocurrency. A type of digital currency that uses encryption techniques for security and anti-counterfeiting measures.

Cybercriminal. Any individual who illegally accesses a computer system or account to damage or steal information.

Device. A computing or communications device. For example, a computer, laptop, mobile phone or tablet.

Digital footprint. The unique set of a user's traceable activities, actions, contributions and communications on the internet or digital devices.

End of support. End of support refers to a situation in which a company ceases support for a product or service. This is typically applied to hardware and software products when a company releases a new version and ends support for previous versions.

Encryption. The process of making data unreadable for the purpose of preventing those without the encryption key (password) from gaining access to its contents.

Internet of Things (IoT). The network of physical objects, devices, vehicles, buildings and other items which are embedded with electronics, software, sensors, and network connectivity, which enables these objects to connect to the internet and collect and exchange data.

IP address. Short for Internet Protocol. A code made up of a string of numbers that identifies a particular computer on the internet. Every computer requires an IP address to connect to the internet.

Factory reset. Restores a device to its original manufacturer settings.

Hotspot. An area where wireless internet access is available to the general public.

Malware. Malicious software used to gain unauthorised access and control of a user's computer, steal information and disrupt or disable networks.

MFA. Remote access. Gain access and control over devices and networks from an offsite location.

Near Field Communication (NFC). Short-range, wireless communication between two compatible devices, allowing them to share data. Examples include Apple Pay and Google Pay.

Network. A collection of computers, servers, network devices, peripherals, or other devices connected to one another to allow the sharing of data.

Operating system. Software installed on a computer's hard drive that enables computer hardware to communicate with and run computer programs. Examples: Microsoft Windows, Apple macOS, iOS, Android.

Physical token. A physical device that can usually fit on a keyring, which generates a security code used to confirm the identity of a computer user using

Software. Commonly referred to as programs, collection of instructions that enable the user to interact with a computer, its hardware or perform tasks.

Spyware. A program designed to covertly gather information about a user's activity on their device.

Trojan. A type of malware that is often disguised as legitimate software, used by cybercriminals to gain access to users' systems.

Virus. A type of malware that spreads on its own by attaching itself to other software, or copying itself across devices and networks.

Universal Plug and Play (UPnP). Allows devices on a network to automatically find and communicate with each other.