


Everyday Cyber Security: Practical Steps for Australians

Have you ever wondered how safe your online life really is? In this course, you'll discover simple, practical actions you can take every day to protect yourself and your loved ones from common cyber threats. You'll learn how to secure your accounts, recognise scams, keep your devices safe, and confidently navigate the digital world—no technical expertise required. Through clear explanations and real-world examples, you'll build the skills and habits needed to stay secure online and help make Australia a safer place for everyone.

- Getting Started: Why Cyber Security Matters Every Day
- Locking the Front Door: Passphrases and Multi-Factor Authentication
- Spotting Trouble: Recognising and Responding to Scams and Phishing
- Keeping Devices Safe: Updates, Antivirus, and Security Settings
- Staying Secure on the Go: Public Wi-Fi and Shared Devices

 **Cyber Safety Conversations: Protecting Your Community**

 **What To Do If Something Goes Wrong: Reporting and Recovery**

Getting Started: Why Cyber Security Matters Every Day



Why Cyber Security Matters Every Day

Welcome to this essential lesson on cyber security. In today's world, technology is part of almost every aspect of our lives—from connecting with loved ones to managing our finances and accessing services. As Australians, we all share the responsibility to protect ourselves and each other online. By understanding the basics of cyber security, you can help make the digital world safer for everyone.

By the end of this lesson, you'll be able to achieve several important goals. These objectives will help you understand your role in staying safe online and protecting those around you.

- 1 Recognise why cyber security is vital in everyday life for all Australians.
- 2 Spot the most frequent risks and scams that can affect anyone online.
- 3 Understand how your actions contribute to your own and your community's online safety.
- 4 Discover simple actions you can take to reduce your risk online.

Cyber Security: Part of Everyday Life

People of all ages and backgrounds use technology in various settings, such as parks, homes, and cafés. Technology is now woven into our daily routines, from checking emails and shopping online to connecting with friends and family. This constant use of digital devices means our personal information is always at risk if we're not careful. That's why cyber security is essential for everyone, no matter your age or experience with technology.

What Makes Cyber Security So Important?

Click through each section below to discover the main reasons why cyber security matters for every Australian. Understanding these key points will help you see the value of staying safe online.

Protecting Personal Information

Our personal details—like names, addresses, and banking information—are valuable to cybercriminals. Protecting this information helps prevent identity theft and keeps our private lives secure.

By being careful with what we share and how we store our data, we reduce the risk of it falling into the wrong hands.

Preventing Financial Loss and Scams —

Online scams and fraud can lead to significant financial loss. Cybercriminals use tricks like fake emails and websites to steal money or sensitive details.

Understanding these risks helps us spot scams early and avoid falling victim to financial fraud.

Keeping Families and Communities Safe —

Good cyber habits don't just protect us—they also keep our families, friends, and communities safe. When we share devices or information, our actions can impact others.

By practising safe behaviours, we help create a safer online environment for everyone around us.

Supporting a Secure Australia —

Every individual's actions add up to a stronger, more secure Australia. When we all take steps to protect ourselves, we help defend our country's digital infrastructure.

Being cyber aware supports national security and helps Australia stay resilient against online threats.

[CONTINUE](#)

Common Online Threats Facing Australians

Online threats are a reality for everyone, no matter your age or how much you use technology. Scammers and cybercriminals target people from all walks of life, using

increasingly clever tactics. Recognising these threats is the first step to protecting yourself and those you care about.

Spotlight on Online Threats

Flip through these cards to learn about some of the most common online threats Australians face. Knowing what to look out for is key to staying safe online.

Phishing

Phishing is when someone pretends to be a trusted organisation to trick you into giving away personal information. Look for suspicious links or requests for details.

Scams

Scams are deceptive schemes designed to steal your money or information. They often use urgent messages or offers that seem too good to be true.

Malware

Malware is harmful software that can infect your device through links, attachments, or downloads. It can steal data or damage your system.

Data Breaches

A data breach happens when personal information is accessed without permission, often leading to identity theft or financial loss.

Every action you take online can help protect yourself, your loved ones, and your community.

CONTINUE

Cyber Safety: A Shared Responsibility

Everyone has a role in maintaining online safety for themselves and others. Engaging in open discussions about cyber safety with family, friends, and community members raises awareness and promotes safer online behaviors. By supporting one another, we collectively make it more difficult for cybercriminals to succeed.

How You Can Make a Difference.

Expand each item below to discover practical ways you can help keep yourself and your community safe online. Small actions can have a big impact.

Talk About Cyber Safety —

Start regular conversations with your family and friends about staying safe online. Sharing tips and experiences helps everyone stay informed about the latest threats and best practices.

Encourage open discussions so that everyone feels comfortable asking questions or sharing concerns.

Model Good Habits —

Lead by example by using strong passphrases, enabling multi-factor authentication, and keeping your devices updated. When others see you practising good cyber habits, they're more likely to follow suit.

Consistent safe behaviour sets a positive standard for your community.

Share Resources and Support —

Share trustworthy information, such as government resources or helpful guides, with those around you. Helping others find reliable advice strengthens everyone's defences.

Offer support to anyone who may be unsure about what to do if they encounter a suspicious message or scam.

Report Incidents —

If you come across a scam or suspicious activity, report it to the appropriate authorities. Reporting helps protect others and allows experts to respond quickly to new threats.

By taking action, you contribute to a safer online environment for all Australians.

CONTINUE

Essential Cyber Safe Actions.

There are simple, practical steps everyone can take to stay safe online. Throughout this course, you'll learn about these actions in detail, so you can confidently protect yourself and help others do the same.

Preview: Your Cyber Safe Toolkit.

Click through each tab to preview the main actions you'll learn about in this course. These steps form the foundation of strong cyber security.

**STRONG
PASSPHRASES**

MULTI-FACTOR
AUTHENTICATION

RECOGNISING SCAMS

DEVICE AND PRIVACY
SETTINGS

Using unique, strong passphrases for every account is one of the most effective ways to protect yourself online. A passphrase is a string of random words that's easy for you to remember but hard for others to guess.

Creating different passphrases for each account helps prevent cybercriminals from accessing your information if one password is compromised.

STRONG
PASSPHRASES

**MULTI-FACTOR
AUTHENTICATION**

RECOGNISING SCAMS

DEVICE AND PRIVACY
SETTINGS

Multi-factor authentication (MFA) adds an extra layer of security to your accounts. It requires you to provide two or more forms of identification before you can log in.

Even if someone gets hold of your password, MFA makes it much harder for them to access your accounts.

**STRONG
PASSPHRASES**

**MULTI-FACTOR
AUTHENTICATION**

RECOGNISING SCAMS

**DEVICE AND PRIVACY
SETTINGS**

Learning to spot scams is crucial for staying safe online. Scams can come in the form of emails, texts, phone calls, or fake websites.

Knowing the warning signs helps you avoid falling victim to fraud and keeps your information secure.

**STRONG
PASSPHRASES**

**MULTI-FACTOR
AUTHENTICATION**

RECOGNISING SCAMS

**DEVICE AND PRIVACY
SETTINGS**

Keeping your devices updated and regularly checking your privacy settings are key steps in protecting your personal information.

Updates fix security gaps, while privacy settings control what information you share and who can see it.

CONTINUE

Check Your Understanding

Now it's time to put your knowledge to the test. Answer the following questions to reinforce what you've learned and see how much you remember about staying safe online.

Why is it important for everyone to practice cyber safe actions every day?

- Because cyber threats can affect anyone, and safe actions help protect personal and community security.
- Only people who use the internet for banking need to worry about cyber security.
- Cyber security is only important for businesses.
- It's not necessary if you have antivirus software.

SUBMIT

Which of the following is an example of a phishing attempt?

- An email pretending to be from your bank asking for your login details.

- Updating your device's software.
- Using a strong passphrase.
- Setting up multi-factor authentication.

SUBMIT

What is one way you can help your family stay safe online?

- Talk regularly about cyber safety and share tips.
- Ignore suspicious messages.
- Share your passwords with family members.
- Use the same passphrase for every account.

SUBMIT

CONTINUE

Key Takeaways.

Cyber security is everyone's responsibility, and small actions each day make a big difference. By understanding the risks, recognising threats, and practising safe habits, you help protect yourself, your loved ones, and your community. Stay alert, stay informed, and remember that your actions matter.

By taking simple steps every day, you're helping to make Australia a safer place for everyone online.

Locking the Front Door: Passphrases and Multi-Factor Authentication



Securing Your Accounts: The First Line of Defence

Welcome to this lesson on protecting your online accounts. Just as you wouldn't leave your front door unlocked, it's vital to secure your digital life. Strong passphrases and multi-factor authentication (MFA) are two of the most effective ways to keep your accounts safe from unwanted visitors. Let's explore how these tools can help you lock your digital front door.

By the end of this lesson, you'll have the practical skills and knowledge to take charge of your account security. These are the key actions and concepts you'll master:

- 1** Learn what makes a passphrase secure and why it matters.
 - 2** Discover how to generate a different passphrase for every account you use.
 - 3** Find out how password managers can help you keep track of your passphrases safely.
 - 4** Gain step-by-step knowledge on enabling MFA for your accounts.
-

See how using both strong passphrases and MFA together offers maximum protection.

Why Strong Passphrases Matter

Weak passwords are like leaving your door unlocked—easy for cybercriminals to break in. Strong passphrases, made up of random words and extra characters, act as a sturdy lock, making it much harder for anyone to access your accounts without permission.

Building a Strong Passphrase.

Expand each section below to learn the essential features of a secure passphrase. These tips will help you create passphrases that are both memorable and hard to crack.

Length and Complexity —

A strong passphrase should be at least 15 characters long and use a sequence of four or more random words. The longer and more complex your passphrase, the harder it is for someone to guess or break it.

Adding extra words or mixing in different types of characters increases your security even further.

Uniqueness for Every Account —

Never use the same passphrase for more than one account. If one account is compromised, reusing passphrases can put all your other accounts at risk.

Unique passphrases ensure that a breach in one place doesn't open the door everywhere else.

Avoiding Personal Information —

Don't include names, birthdays, addresses, or any details that someone could easily find out about you. Personal information makes it easier for cybercriminals to guess your passphrase.

Stick to random words and avoid anything that relates directly to your life.

Adding Symbols and Numbers —

Some websites require symbols, capital letters, or numbers. Add these in creative ways, but don't rely on them alone for strength.

Mixing in different character types can help meet requirements and make your passphrase even stronger.

CONTINUE

Managing Your Passphrases.

As you create unique passphrases for each account, it can be tricky to remember them all. That's where password managers come in—they help you securely store and organise your passphrases, so you don't have to rely on memory alone. Keeping your passphrases safe and accessible is just as important as creating them.

Ways to Manage Your Passphrases.

Explore the tabs below to compare different methods for keeping track of your passphrases. Each approach has its own benefits and considerations.

MEMORY TRICKS

PASSWORD MANAGERS

WRITTEN RECORDS

Using memorable but random word sequences can help you recall your passphrases without writing them down. Try creating a story or image in your mind that links the words together.

This method works best for a few accounts, but can become difficult as the number grows.

MEMORY TRICKS

PASSWORD MANAGERS

WRITTEN RECORDS

Password managers are secure apps or programs that generate, store, and fill in your passphrases for you. They can also alert you if a passphrase has been compromised in a data breach.

Using a reputable password manager means you only need to remember one strong master passphrase.

MEMORY TRICKS

PASSWORD MANAGERS

WRITTEN RECORDS

Some people choose to write their passphrases in a notebook kept in a safe place. This can be a practical backup, especially if you're not comfortable with digital tools.

However, written records must be stored securely and never left where others can find them.

Never use the same passphrase for more than one account.

If one account is breached, all your accounts using that passphrase could be at risk.

Adding Another Lock: Multi-Factor Authentication

Imagine a person holding their phone and reading a verification code while logging in on their computer. Multi-factor authentication (MFA) acts like adding a second lock to your digital door. It requires you to provide two or more ways to prove your identity, making it much harder for anyone else to access your accounts—even if they know your passphrase.

How Multi-Factor Authentication Works.

Expand each item below to learn how MFA protects your accounts and how you can set it up. These steps will help you add an extra layer of security to your digital life.

What is MFA?

MFA stands for multi-factor authentication. It means you need to provide two or more types of identification to access your account, such as something you know (your passphrase) and something you have (a code sent to your phone).

This extra step makes it much harder for cybercriminals to break in, even if they have your passphrase.

Common MFA Methods

Common MFA methods include SMS codes sent to your phone, authenticator apps that generate time-based codes, and email verification codes.

Some services also use biometric methods, like fingerprints or facial recognition, for even more security.

Setting Up MFA —

To enable MFA, go to your account's security settings and look for the option to add multi-factor authentication. Follow the prompts to link your phone number, email, or authenticator app.

Once set up, you'll be asked for a code or other proof each time you log in from a new device.

Troubleshooting and Tips —

If you lose access to your phone or authenticator app, most services offer backup codes or alternative methods to regain access. Store these backup options in a safe place.

Always keep your contact details up to date to avoid being locked out of your accounts.

CONTINUE

Double Up for Maximum Protection.

Using both strong, unique passphrases and multi-factor authentication together creates a powerful barrier against cyber threats. Even if someone manages to get your passphrase, MFA adds another hurdle, making it extremely difficult for anyone else to access your accounts. Combining these tools is the best way to keep your digital life secure.

Quick Review: Secure Account Habits.

Flip through these cards to reinforce the best practices for protecting your accounts.

Remember, these habits make a real difference in your online safety.

Strong Passphrase

A strong passphrase uses 15+ characters and random words, like: "RiverSunshineCoffeeTrain".

Unique for Every Account

Each account should have its own passphrase. This way, a breach in one place doesn't affect others.

Multi-Factor Authentication

MFA requires two or more proofs of identity, making it much harder for cybercriminals to access your accounts.

Password Manager

A password manager securely stores and fills in your passphrases, so you don't have to remember them all.

CONTINUE

Check Your Understanding

Test your knowledge with the following questions. Answering them will help you remember the key points about securing your accounts with strong passphrases and MFA.

Which of the following is the best example of a strong passphrase?

- BlueAppleRiverSunshine
- JohnSmith1980
- Password123!
- Sydney2022

SUBMIT

Why should you avoid using the same passphrase for multiple accounts?

- If one account is breached, others could be compromised too.
- It's easier to remember different passphrases.

- Websites require different passphrases.
- It makes logging in faster.

SUBMIT

What does multi-factor authentication add to your account security?

- It requires extra proof of identity, making it harder for others to access your account.
- It makes your passphrase longer.
- It automatically updates your passwords.
- It lets you share accounts safely.

SUBMIT

CONTINUE

Key Takeaways.

Strong, unique passphrases and multi-factor authentication are your best defences against online threats. By combining these tools, you make it much harder for anyone to access your accounts without your permission. Take charge of your digital security—these simple steps make a big difference.

Lock your digital front door by protecting your accounts with strong passphrases and multi-factor authentication. These measures help keep your information secure from unauthorized access.

Spotting Trouble: Recognising and Responding to Scams and Phishing



Stay Alert: Spotting Scams and Phishing Attempts

Welcome to this lesson on recognising and responding to scams and phishing. Scams and phishing attempts are increasingly common in Australia, targeting people from all backgrounds. Learning how to spot and deal with these threats is essential for protecting yourself, your loved ones, and your community online.

By the end of this lesson, you'll be equipped with practical skills to identify and respond to scams and phishing attempts. Here's what you'll be able to do:

- 1** Recognise different forms of scams and phishing attempts you may encounter online or by phone.
 - 2** Learn to notice the red flags that signal a message or offer might be a scam.
 - 3** Know how to double-check if a message or request is genuine before responding.
 - 4** Understand the safest actions to take if you suspect a scam or phishing attempt.
-

Scams and Phishing: A Growing Threat

Scams and phishing are becoming more sophisticated and widespread, affecting Australians from all walks of life. Cybercriminals use clever tricks to steal information or money, so it's important to stay informed and cautious.

Common Types of Scams and Phishing.

Expand each item below to learn about the most frequent scams and phishing tactics. Understanding these types will help you stay one step ahead.

Phishing Emails and Messages

Phishing involves emails or messages that pretend to be from trusted organisations, asking you to click links or provide personal information. These messages often look official but are designed to steal your details.

Be wary of unexpected requests for information, especially if they urge you to act quickly or click a link.

Fake Websites and Ads

Scammers create fake websites and online ads that look real to trick you into entering your details or making payments. These sites may use logos and designs that closely mimic legitimate businesses.

Always check website addresses carefully and avoid clicking on ads that seem suspicious or too good to be true.

Phone and SMS Scams —

Phone and SMS scams involve calls or texts from people pretending to be from banks, government agencies, or companies. They may ask for personal details, payment, or try to scare you into acting quickly.

Never share sensitive information over the phone or by text unless you are certain of the caller's identity.

Social Media and Impersonation —

Some scams use social media to impersonate friends, family, or well-known organisations. You might receive messages from fake accounts asking for money or personal information.

Be cautious with unexpected requests on social media, even if they appear to come from someone you know.

CONTINUE

Warning Signs: How to Spot a Scam

Scams and phishing attempts often share common warning signs. Being alert to these red flags can help you avoid falling victim. Watch for anything unusual or unexpected in messages, calls, or online offers.

Red Flags to Watch For.

Click through each tab to learn about the key warning signs of scams and phishing. Recognising these can help you stay safe online.

**PRESSURE TO ACT
QUICKLY**

**TOO GOOD TO BE
TRUE OFFERS**

**UNUSUAL PAYMENT
REQUESTS**

**LINKS AND
ATTACHMENTS**

Scammers often try to rush you into making a decision. They may claim your account is at risk or offer a deal that expires soon.

Take your time and don't let anyone pressure you into acting before you've checked the facts.

**PRESSURE TO ACT
QUICKLY**

**TOO GOOD TO BE
TRUE OFFERS**

**UNUSUAL PAYMENT
REQUESTS**

**LINKS AND
ATTACHMENTS**

Be wary of offers that promise large sums of money, prizes, or amazing deals. If it sounds too good to be true, it probably is.

Scammers use these tactics to lure you in and get your personal details or money.

**PRESSURE TO ACT
QUICKLY**

**TOO GOOD TO BE
TRUE OFFERS**

**UNUSUAL PAYMENT
REQUESTS**

**LINKS AND
ATTACHMENTS**

Requests for payment using gift cards, cryptocurrency, or setting up new accounts are a major red flag. Legitimate organisations rarely ask for payment in these ways.

If you're asked to pay in an unusual way, double-check before proceeding.

PRESSURE TO ACT
QUICKLY

TOO GOOD TO BE
TRUE OFFERS

UNUSUAL PAYMENT
REQUESTS

LINKS AND
ATTACHMENTS

Unsolicited emails or messages with links or attachments can be dangerous. These may lead to fake websites or install malware on your device.

Don't click on links or open attachments unless you're sure they're safe.

If something feels off, it probably is. Trust your instincts and take the time to double-check.

CONTINUE

Verify Before You Trust

Before you respond or click on anything, it's important to double-check who you're really communicating with. Taking a moment to verify can prevent you from falling for a scam. For example, you might use your computer to look up the sender of a message you received on your phone. Always take the time to confirm the identity of the sender before taking any action.

What To Do If You Suspect a Scam.

Expand each item below for practical advice on how to respond if you think you've encountered a scam or phishing attempt.

Stop and Think —

Pause before responding to any unexpected message or request. Scammers rely on you acting quickly without thinking.

Taking a moment to consider the situation can help you avoid making a mistake.

Check the Source —

Don't trust contact details in the suspicious message. Instead, find official contact information from a trusted website or source and reach out directly.

This helps you confirm if the request is genuine or a scam.

Don't Click or Share —

Avoid clicking on any links or sharing personal information until you're sure the message is legitimate. Scammers use links to steal your details or install malware.

If in doubt, delete the message or contact the organisation using a method you trust.

Protect and Report —

If you think you've been targeted or have shared information, act quickly. Change your passwords, contact your bank if money is involved, and report the scam to authorities like Scamwatch.

Reporting helps protect others and can stop scammers from targeting more people.

CONTINUE

Reporting Scams and Cyber Incidents

Reporting scams and cyber incidents is vital for protecting yourself and your community. When you report, you help authorities track new threats and warn others, making it harder for scammers to succeed.

Quick Review: Responding and Reporting.

Flip through these cards to reinforce the best ways to respond to scams and phishing. Remember, your actions can help protect others as well as yourself.

Who to Contact

If you suspect a scam, contact your bank, Scamwatch, or the relevant organisation immediately.

What to Report

Include details like the message, sender, what was asked, and any links or attachments when reporting.

Why Reporting Matters

Reporting helps authorities warn others and stop scammers from targeting more people.

Immediate Actions

If you've shared information or lost money, change your passwords and contact your bank right away.

CONTINUE

Check Your Understanding

Test your knowledge with the following questions. Answering them will help you remember the key points about spotting, responding to, and reporting scams and phishing attempts.

Which of the following is an example of a phishing attempt?

- An email pretending to be your bank asking for your login details.

- A friend calling to chat about your weekend.
- A reminder from your calendar app.
- A news article from a trusted website.

SUBMIT

Which of these is a warning sign of a scam?

- Being pressured to act quickly.
- A message from a known contact with no requests.
- A regular bill from your utility company.
- A social media post from a friend.

SUBMIT

What should you do if you receive a suspicious message?

- Don't click any links, verify the sender, and report it if needed.
- Reply to the message to ask for more details.
- Ignore it and hope it goes away.
- Forward it to friends to warn them.

SUBMIT

CONTINUE

Key Takeaways.

Staying alert to scams and phishing is vital for your safety online. By recognising common tactics, spotting warning signs, and knowing how to respond and report, you help protect yourself and your community. Remember, a little caution goes a long way.

Your awareness is your best defence—stay sharp and help protect your community.

Keeping Devices Safe: Updates, Antivirus, and Security Settings



Protecting Your Devices: The Foundation of Cyber Safety.

Welcome to this lesson on keeping your devices secure. Your phone, computer, and tablet are gateways to your personal information and daily life. Keeping them safe and up to date is the foundation for all other cyber security actions, helping you protect your privacy and stay ahead of online threats.

By the end of this lesson, you'll have the skills and confidence to keep your devices secure. Here are the key actions and knowledge you'll gain:

- 1** Learn why installing updates promptly is crucial for device security.
 - 2** Find out how to set up and maintain antivirus software on your devices.
 - 3** Discover how to turn on built-in security settings for extra protection.
-

4

Explore how to control what information your devices and apps share.

5

Learn how to adjust location settings to safeguard your privacy.

Why Updates and Security Matter

Software updates and security features are your first defence against new cyber threats. They fix weaknesses that cybercriminals might exploit, making it much harder for anyone to access your information without your permission.

The Benefits of Keeping Devices Updated.

Expand each section below to learn why regular updates and security features are so important for your devices.

Fixing Security Flaws —

Updates patch vulnerabilities that could let cybercriminals into your device. Without these fixes, your device is more exposed to attacks.

Installing updates as soon as they're available helps close these security gaps quickly.

Protecting Personal Data —

Regular updates help keep your personal information safe from hackers. They strengthen your device's defences and reduce the risk of data theft.

Protecting your data means protecting your identity, finances, and privacy.

Improving Device Performance —

Updates often include improvements that make your device run smoother and more reliably. They can fix bugs and boost speed.

Keeping your device updated ensures you get the best performance and fewer problems.

Staying Ahead of Cybercriminals —

Cyber threats are always evolving. Updates help your device stay one step ahead by defending against the latest tricks and attacks.

Turning on automatic updates is a simple way to keep your protection current.

CONTINUE

Antivirus Software: Your Digital Shield.

Antivirus software acts as a protective barrier for your devices. It scans for, detects, and removes malicious software (malware) that could steal your information or damage your device. Every device—whether it's a phone, tablet, or computer—should have antivirus protection to reduce the risk of infection from viruses, ransomware, and other threats.

Understanding Antivirus Protection.

Click through the tabs below to learn about the essentials of antivirus software and how to get the most out of it.

**WHAT ANTIVIRUS
DOES**

**BUILT-IN VS.
PURCHASED**

**KEEPING ANTIVIRUS
UPDATED**

AUTOMATIC SCANS

Antivirus software scans your device for harmful programs and blocks or removes them before they can cause damage. It helps protect your personal data and keeps your device running smoothly.

It also warns you about suspicious files or websites, giving you a chance to avoid threats.

**WHAT ANTIVIRUS
DOES**

**BUILT-IN VS.
PURCHASED**

**KEEPING ANTIVIRUS
UPDATED**

AUTOMATIC SCANS

Many devices come with built-in antivirus protection, but you can also buy third-party antivirus programs for extra features. Both options can be effective if kept up to date.

Choose the solution that best fits your needs and make sure it's always active.

**WHAT ANTIVIRUS
DOES**

**BUILT-IN VS.
PURCHASED**

**KEEPING ANTIVIRUS
UPDATED**

AUTOMATIC SCANS

Regular updates are essential for antivirus software to recognise new threats. Set your antivirus to update automatically so it always has the latest protection.

Outdated antivirus can't defend against the newest viruses or malware.

WHAT ANTIVIRUS
DOES

BUILT-IN VS.
PURCHASED

KEEPING ANTIVIRUS
UPDATED

AUTOMATIC SCANS

Set your antivirus to run regular scans automatically. This helps catch threats early, even if you haven't noticed anything unusual.

Automatic scans give you peace of mind that your device is being checked regularly.

An up-to-date antivirus program is your first line of defence against online threats.

CONTINUE

Take Control of Your Privacy

Imagine someone adjusting privacy settings on their smartphone or social media account. Regularly reviewing your privacy and location settings allows you to manage what information your devices and apps share. Taking this step is essential for safeguarding your personal data from unauthorized access or misuse.

How to Manage Privacy and Location Settings.

Expand each item below for practical steps to keep your information private and secure.

Review Privacy Settings —

Check the privacy options on your devices and online accounts. Adjust who can see your information and what data is shared.

Review these settings regularly, especially after updates or installing new apps.

Limit Profile Visibility —

Restrict your profile visibility to trusted friends and family. Avoid sharing personal details with the public or strangers.

This helps prevent cybercriminals from gathering information about you.

Disable Unnecessary Location Access —

Turn off location tracking for apps and devices that don't need it. Most apps work fine without knowing your location.

Check your device settings to see which apps have access and adjust as needed.

Control Camera and Photo Access —

Some apps ask for access to your camera and photos. Only allow this if it's necessary for the app to work.

Review and update these permissions regularly to keep your private images secure.

CONTINUE

Make Device Security a Habit.

Device security isn't a one-time task—it's an ongoing habit. Set reminders to check for updates, use automatic updates where possible, and regularly review your security and privacy settings. These small steps help keep your devices and information safe every day.

Quick Review: Device Safety Habits.

Flip through these cards to reinforce the best practices for keeping your devices secure. Remember, a few simple habits can make a big difference.

Why Update Regularly?

Updates fix security flaws and protect your device from new threats.

Antivirus Essentials

Keep your antivirus updated and run regular scans for the best protection.

Privacy Settings

Review privacy options often to control who can see your information.

Location Controls

Manage which apps can access your location to protect your privacy.

CONTINUE

Check Your Understanding

Test your knowledge with the following questions. Answering them will help you remember the key points about keeping your devices safe and secure.

What is one main benefit of keeping your devices updated?

- It fixes security flaws that could be exploited by cybercriminals.
- It makes your device look newer.

It increases your device's storage space.

It automatically deletes old files.

SUBMIT

Which of the following is a best practice for antivirus software?

Keep it updated and run regular scans.

Turn it off when not online.

Only use it on your computer, not your phone.

Update it once a year.

SUBMIT

How can you protect your privacy on social media and devices?

-
- Review and adjust privacy and location settings regularly.
 - Share your location with everyone.
 - Accept all app permissions without checking.
 - Never update your privacy settings.

SUBMIT

CONTINUE

Key Takeaways.

Keeping your devices safe is the foundation of cyber security. Regular updates, strong antivirus protection, and careful privacy management all work together to protect your information and give you peace of mind. Make these habits part of your routine for lasting security.

A few simple habits can help keep your devices and information safe every day.

Staying Secure on the Go: Public Wi-Fi and Shared Devices



Staying Safe on Public Wi-Fi and Shared Devices.

Welcome to this lesson on staying secure while you're out and about. Using public Wi-Fi or shared devices is convenient, but it also introduces new risks to your personal information. Learning safe habits for these situations is essential for protecting yourself in everyday life, whether you're at a café, airport, or sharing a device with someone else.

By the end of this lesson, you'll know how to protect yourself when using public networks or devices that aren't your own. Here are the key skills and actions you'll master:

- 1** Learn why public networks can be unsafe and what dangers to watch for.
 - 2** Discover how to browse securely and avoid exposing sensitive information on public Wi-Fi.
 - 3** Find out how to keep your data private in public spaces and on shared devices.
-

The Hidden Risks of Public Networks

Imagine people working on laptops and smartphones in a bustling café or airport lounge. While public Wi-Fi networks offer convenience, they also present significant security risks. Cybercriminals often target these networks to steal personal information or intercept sensitive data. Without taking proper precautions, your private details could be exposed every time you connect to a public network.

What Makes Public Wi-Fi and Shared Devices Risky?

Expand each section below to learn about the most common dangers of using public networks and shared devices.

Unsecured Connections —

Most public Wi-Fi networks don't use encryption, meaning the information you send and receive isn't protected. This makes it easier for others to intercept your data.

Always assume that anything you do on public Wi-Fi could be visible to others on the same network.

Eavesdropping and Data Theft —

Cybercriminals can use special tools to eavesdrop on public networks, capturing passwords, messages, or other sensitive information you send.

Be cautious about what you access or share when connected to public Wi-Fi.

Malware and Fake Networks

Some attackers set up fake Wi-Fi hotspots or infect public networks with malware. Connecting to these can put your device and data at risk.

Only connect to networks you trust and avoid downloading files or apps while on public Wi-Fi.

Shared Device Pitfalls

Using a device that isn't yours—like a public computer or a friend's phone—means you can't be sure how secure it is. Saved passwords, browsing history, or malware could compromise your privacy.

Always be extra careful and avoid accessing sensitive accounts on shared devices.

CONTINUE

Safe Browsing on Public Wi-Fi.

When you use public Wi-Fi, it's important to be proactive about your safety. Treat every public network as potentially unsafe and take steps to protect your information. With the right habits, you can reduce your risk and browse with greater confidence.

Top Tips for Public Wi-Fi Safety.

Click through the tabs below to learn essential habits for staying safe on public Wi-Fi. These tips will help you keep your information secure, even in busy public places.

**AVOID SENSITIVE
ACTIVITIES**

**USE SECURE
WEBSITES**

TURN OFF SHARING

**FORGET THE
NETWORK**

Don't access online banking, email, or other sensitive accounts while on public Wi-Fi. Wait until you're on a secure, private network to handle important tasks.

This reduces the risk of your information being intercepted by cybercriminals.

**AVOID SENSITIVE
ACTIVITIES**

**USE SECURE
WEBSITES**

TURN OFF SHARING

**FORGET THE
NETWORK**

Always check for HTTPS in the website address before entering any information. Secure websites encrypt your data, making it harder for others to steal it.

Look for the padlock icon in your browser's address bar as a sign of a secure connection.

**AVOID SENSITIVE
ACTIVITIES**

**USE SECURE
WEBSITES**

TURN OFF SHARING

**FORGET THE
NETWORK**

Disable file and device sharing features on your device before connecting to public Wi-Fi. This prevents others on the network from accessing your files or device.

You can usually find these settings in your device's network or sharing options.

**AVOID SENSITIVE
ACTIVITIES**

**USE SECURE
WEBSITES**

TURN OFF SHARING

**FORGET THE
NETWORK**

After using public Wi-Fi, disconnect and remove the network from your device's list of known networks. This stops your device from reconnecting automatically in the future.

Forgetting the network helps you stay in control of your connections.

If you wouldn't shout something in a public place, you shouldn't share it over public Wi-Fi. Information sent over public networks can be easily intercepted, so avoid sharing sensitive or personal details when connected to unsecured Wi-Fi.

CONTINUE

Keep Your Information Private

Imagine someone using a privacy filter on their laptop or shielding their phone screen from prying eyes in a public space. It's important to be discreet with your personal and financial information when you're out and about. Simple actions, such as covering your screen or using privacy settings, can help keep your data safe from others nearby.

How to Stay Safe on Shared Devices.

Expand each item below for practical steps to protect your information when using devices that aren't your own.

Log Out of Accounts —

Always log out of your accounts when you're finished, especially on shared or public devices. This prevents others from accessing your information after you leave.

Double-check that you've signed out of all apps and websites before closing the browser or leaving the device.

Don't Save Passwords —

Never allow a shared device to save your passwords or login details. If prompted, choose 'No' or 'Never' when asked to save credentials.

This helps ensure your accounts remain secure, even if someone else uses the device later.

Clear Browsing Data —

After using a shared device, clear the browsing history, cookies, and cache. This removes traces of your activity and helps protect your privacy.

Most browsers have an option to clear data in their settings or history menu.

Use Private Browsing —

Whenever possible, use incognito or private browsing modes. These modes don't save your browsing history or login details after you close the window.

It's an extra layer of privacy when you can't avoid using a shared device.

CONTINUE

Make Security a Habit—Wherever You Are.

Good security habits don't stop when you leave home. Stay alert when using public networks or devices, and use trusted devices for sensitive activities whenever possible. Regularly review your habits to make sure you're always protecting your information, no matter where you are.

Quick Review: Security on the Go.

Flip through these cards to reinforce the best practices for staying secure on public Wi-Fi and shared devices. These habits will help you protect your information wherever you go.

Why Avoid Sensitive Tasks on Public Wi-Fi?

Public Wi-Fi is often unsecure, making it easy for others to intercept your data or steal your information.

Best Practice After Using a Shared Device

Always log out of accounts and clear browsing data to protect your privacy.

How to Spot an Unsecure Network

Unsecure networks may not require a password or use encryption. Be cautious if you're not sure who owns the network.

What to Do If You Suspect a Breach

Change your passwords, monitor your accounts, and seek help if you think your information was compromised.

CONTINUE

Check Your Understanding

Test your knowledge with the following questions. Answering them will help you remember the key points about staying secure on public Wi-Fi and shared devices.

What is a main risk of using public Wi-Fi?

- Cybercriminals can intercept your information.
- Your device will run out of battery faster.

- Websites will load more slowly.
- You'll get more pop-up ads.

SUBMIT

Which is a safe habit when using public Wi-Fi?

- Avoid accessing sensitive accounts like banking or email.
- Save your passwords in the browser.
- Leave file sharing turned on.
- Stay connected to public Wi-Fi all day.

SUBMIT

What should you do after using a shared device?

-
- Log out of all accounts and clear browsing data.
 - Leave your accounts logged in for convenience.
 - Save your passwords for next time.
 - Do nothing—shared devices are always safe.

SUBMIT

CONTINUE

Key Takeaways.

Staying secure on the go means being cautious with public Wi-Fi and shared devices. By understanding the risks and following safe habits, you can protect your information wherever you are. Make these practices part of your routine for peace of mind every day.

Stay alert on the go—your information is worth protecting,
wherever you are.

Cyber Safety Conversations: Protecting Your Community



Cyber Safety Starts with a Conversation.

Welcome to this lesson on the power of talking about cyber safety. Open, supportive discussions about online security help protect not just you, but also your friends, family, and the wider community. By sharing knowledge and experiences, we can all play a part in building a safer digital world together.

By the end of this lesson, you'll be ready to make a real difference in your community's online safety. Here are the key skills and actions you'll develop:

- 1 Recognise why discussing cyber safety helps protect everyone around you.
- 2 Learn practical ways to begin cyber safety conversations with different people.
- 3 Find out how to provide trusted information and assistance to others.
- 4 Discover how to support and motivate others to stay secure online.

Why Cyber Safety Conversations Matter

Sharing knowledge and experiences about online safety can help prevent cyber incidents and create a safer environment for everyone. When we talk openly, we empower each other to make better decisions and avoid common online pitfalls. Whether it's a family at the kitchen table, friends at a café, or colleagues in a meeting, discussing cyber safety is essential for all age groups and settings.

The Power of Talking About Cyber Safety.

Expand each section below to discover the many benefits of having open conversations about online safety. These discussions can have a positive impact on everyone involved.

Raising Awareness —

Talking about cyber safety helps others recognise risks they might not have noticed. Awareness is the first step to prevention.

When people know what to look out for, they're less likely to fall for scams or make risky choices online.

Preventing Mistakes —

Sharing tips and real-life stories can help others avoid common online mistakes. Learning from each other's experiences is powerful.

Open conversations can stop problems before they start.

Supporting Recovery —

If someone experiences a cyber incident, talking about it can help them recover and learn from the situation. It's important to know you're not alone.

Supportive discussions can provide comfort and practical advice for moving forward.

Building a Safer Community —

When everyone shares knowledge and looks out for each other, the whole community becomes stronger and safer online.

Collective action makes it harder for cybercriminals to succeed.

CONTINUE

How to Start the Conversation.

Approaching cyber safety discussions in a supportive, non-judgmental way is key. Whether you're talking to family, friends, or colleagues, being open and understanding encourages others to share and learn. Remember, everyone's experience with technology is different, so patience and empathy go a long way.

Conversation Starters for Every Situation.

Click through the tabs below to discover practical ways to begin cyber safety conversations with different people in your life. Tailoring your approach helps make these talks more effective and comfortable.

WITH FAMILY

WITH FRIENDS

WITH CHILDREN OR
TEENS

WITH OLDER ADULTS

Bring up online safety during everyday activities, like dinner or while watching TV. Ask questions like, 'Have you seen any strange messages lately?' or 'Do you know how to check your privacy settings?'

Keep the tone light and supportive, making it easy for everyone to join in.

WITH FAMILY

WITH FRIENDS

WITH CHILDREN OR
TEENS

WITH OLDER ADULTS

Share a recent news story or personal experience as a conversation starter. For example, 'I heard about a new scam going around—have you seen it?'

Offer tips casually and encourage friends to share their own experiences.

WITH FAMILY

WITH FRIENDS

**WITH CHILDREN OR
TEENS**

WITH OLDER ADULTS

Use age-appropriate language and examples. Ask about their favourite apps or games, and talk about how to stay safe while using them.

Listen to their concerns and make sure they feel comfortable asking questions.

WITH FAMILY

WITH FRIENDS

WITH CHILDREN OR
TEENS

WITH OLDER ADULTS

Be respectful and clear. Offer to help check settings or explain new threats in simple terms. For example, 'Would you like me to show you how to spot scam emails?'

Reassure them that it's okay to ask for help and that everyone can learn something new.

A simple conversation can have a significant impact on someone's online safety.

CONTINUE

Sharing Resources and Support

Imagine someone assisting another person with a digital device, such as showing them how to change a setting or sharing a useful website on a screen. By providing reliable resources and offering practical help, you empower others to take action and boost their confidence in managing their online safety.

Ways to Support Safe Online Habits.

Expand each item below for practical ways to help others stay secure online. These actions can make a real difference in your community.

Share Trusted Websites —

Recommend official government or reputable cyber safety websites for up-to-date advice. Sharing reliable sources helps others find accurate information quickly.

Encourage people to bookmark these sites for easy access.

Offer to Help Set Up Security —

Offer hands-on help with setting up security features, like strong passphrases or privacy settings. Sometimes, a little guidance is all someone needs to feel secure.

Be patient and explain each step clearly.

Discuss Recent Scams —

Talk about new scams or threats you've heard about in the news or from friends. Sharing this information keeps everyone alert and prepared.

Encourage others to share what they've seen, too.

Encourage Reporting —

Remind people that reporting suspicious activity or cyber incidents is important. Support them in knowing where and how to report issues.

Reporting helps protect the whole community and can prevent further harm.

CONTINUE

Encouraging Safe Habits in Others.

Supporting others in building safe online habits is an ongoing process. Model good behaviour, check in regularly, and celebrate progress together. By making cyber safety a shared goal, you help create a culture of security and trust in your community.

Quick Review: Supporting Your Community.

Flip through these cards to reinforce the best ways to help your community stay safe online. These habits make a real difference for everyone.

Why Talk About Cyber Safety?

Open conversations raise awareness, prevent mistakes, and help everyone feel supported online.

How to Start the Conversation

Be supportive, patient, and tailor your approach to the person you're talking to.

Sharing Resources

Share official websites, guides, and offer hands-on help with settings or updates.

Encouraging Good Habits

Model safe behaviour, check in regularly, and celebrate progress with others.

CONTINUE

Check Your Understanding

Test your knowledge with the following questions. Answering them will help you remember the key points about supporting your community through cyber safety conversations and actions.

What is one benefit of discussing cyber safety with others?

- It helps raise awareness and prevent mistakes.

- It makes online threats more likely.
- It only helps people who are experts.
- It's not necessary if you use antivirus software.

SUBMIT

What is a good way to start a cyber safety conversation with a friend or family member?

- Share a recent news story or ask about their experiences.
- Criticise their online habits immediately.
- Avoid talking about technology altogether.
- Only talk about cyber safety if there's a problem.

SUBMIT

How can you encourage others to adopt safe online habits?

- Model good behaviour and check in regularly.
- Ignore their questions about security.
- Only share resources once.
- Tell them to figure it out themselves.

SUBMIT

CONTINUE

Key Takeaways.

Open conversations and community support are powerful tools for building a safer online environment. By sharing knowledge, offering help, and encouraging good habits, you help protect not just yourself but everyone around you. Make cyber safety a regular topic in your community for lasting impact.

Together, we can make cyber safety a habit for everyone.

What To Do If Something Goes Wrong: Reporting and Recovery



When Things Go Wrong: Taking Action After a Cyber Incident.

Welcome to this important lesson on what to do if you experience a cyber incident. Remember, anyone can fall victim to scams, hacking, or data loss—what matters most is knowing how to respond. Taking the right steps can help you recover quickly and protect yourself and others in the future.

By the end of this lesson, you'll be prepared to act confidently if something goes wrong online. Here are the key skills and actions you'll master:

- 1 Know when to report:** Recognise situations where reporting a cyber incident is necessary and urgent.
 - 2 How to report in Australia:** Understand the process for reporting scams and cybercrime to the right authorities.
 - 3 What happens after reporting:** Learn what to expect once you've submitted a report and how follow-up works.
-

Steps for recovery: Identify practical actions to regain control and protect yourself after an incident.

You're Not Alone: Support Is Available

Imagine an image of someone sitting at their desk, talking on the phone with a support representative, or a comforting hand on their shoulder. Cyber incidents can happen to anyone, regardless of age or experience. Reaching out for help is a sign of strength, and there are many services and people ready to support you through recovery.

When and Why Should You Report?

Expand each section below to learn about the importance of reporting cyber incidents promptly. Timely action can make a big difference for you and your community.

If You Lose Money or Personal Information —

If you've lost money or shared sensitive details, report the incident immediately. Quick reporting increases the chance of recovering funds and limiting further damage.

Contact your bank or relevant service provider as soon as possible.

If You Notice Suspicious Activity —

Even if you're not sure, report any unusual account activity or unexpected messages. Early reporting can help stop a scam before it causes harm.

Trust your instincts—if something feels off, it's worth checking.

To Help Others and the Community —

Reporting scams and cybercrime helps authorities warn others and prevent similar incidents. Your action could protect friends, family, and the wider community.

Sharing your experience can also raise awareness and help others stay safe.

To Aid Recovery —

Reporting is often the first step in getting help to recover lost money or secure your accounts. Authorities and support services can guide you through the recovery process.

Don't hesitate to ask for assistance—it's there for you.

CONTINUE

How to Report Scams and Cybercrime.

Knowing where and how to report a cyber incident is crucial. In Australia, there are dedicated organisations and services to help you respond to scams, fraud, and cyber attacks. Acting quickly and providing the right information can make a real difference in resolving the issue.

Reporting Channels and What to Include.

Click through each tab to learn about the main ways to report a cyber incident and what information you should provide. Each channel is designed to help you in different situations.

BANK OR FINANCIAL INSTITUTION	SCAMWATCH	AUSTRALIAN SIGNALS DIRECTORATE	OTHER SUPPORT SERVICES
--------------------------------------	------------------	---------------------------------------	-------------------------------

If you've lost money or suspect fraud, contact your bank or financial provider immediately. They can freeze accounts, reverse transactions, and offer advice.

Be ready to provide details of the incident, including dates, amounts, and any suspicious messages.

BANK OR FINANCIAL INSTITUTION	SCAMWATCH	AUSTRALIAN SIGNALS DIRECTORATE	OTHER SUPPORT SERVICES
--------------------------------------	------------------	---------------------------------------	-------------------------------

Report scams to Scamwatch, the Australian government's scam reporting service. Include as much detail as possible—what happened, how you were contacted, and any evidence like emails or screenshots.

Scamwatch uses this information to warn others and track scam trends.

BANK OR FINANCIAL INSTITUTION	SCAMWATCH	AUSTRALIAN SIGNALS DIRECTORATE	OTHER SUPPORT SERVICES
--------------------------------------	------------------	---------------------------------------	-------------------------------

For serious cybercrime or attacks, report to the Australian Signals Directorate (ASD). They handle incidents like hacking, ransomware, and large-scale breaches.

Provide technical details if possible, such as device type, affected accounts, and what actions you've taken.

BANK OR FINANCIAL INSTITUTION	SCAMWATCH	AUSTRALIAN SIGNALS DIRECTORATE	OTHER SUPPORT SERVICES
--------------------------------------	------------------	---------------------------------------	-------------------------------

Depending on the situation, you may also contact the police, IDCARE (for identity theft), or support hotlines for advice and assistance.

These services can help you recover and provide emotional support if needed.

The sooner you report, the sooner you can get help and protect others.

CONTINUE

What Happens After You Report?

Once you've reported a cyber incident, you may receive updates, requests for more information, or advice on next steps. Support services are available to guide you through the process and help you recover. For example, you might receive a confirmation email after submitting your report, or take notes during a follow-up call. These steps ensure you are kept informed and supported throughout the resolution process.

After Reporting: What to Expect.

Expand each item below to learn about the typical steps and support you may receive after reporting a cyber incident. Knowing what to expect can help you feel more in control.

Confirmation and Case Number

After reporting, you'll usually receive a confirmation and a case number. Keep this information safe—it helps track your case and makes follow-up easier.

Use your case number when contacting support or checking on progress.

Follow-Up Actions —

You may be asked for more information or to take certain steps, such as changing passwords or monitoring your accounts. Respond promptly to any requests from authorities or support services.

Staying engaged helps resolve the issue faster.

Support and Resources —

Many organisations offer resources, advice, and emotional support after a cyber incident. Take advantage of these services—they're there to help you recover.

Don't hesitate to ask questions or seek further guidance.

Protecting Yourself Going Forward —

After an incident, you'll receive advice on securing your accounts and devices to prevent future problems. This might include enabling extra security features or reviewing your privacy settings.

Learning from the experience helps you stay safer in the future.

CONTINUE

Steps to Recover from a Cyber Incident.

Taking action after a cyber incident is vital for regaining control and confidence. Simple steps such as updating passwords, monitoring your accounts, and seeking support can help you recover and reduce the risk of further harm. Remember, recovery is a process, and help is available every step of the way.

Quick Review: Recovering After an Incident.

Flip through these cards to reinforce the best practices for recovering after a cyber incident. These actions can help you regain control and move forward with confidence.

Change Your Passwords

Update passwords for all affected accounts to stop unauthorised access and strengthen your security.

Monitor Your Accounts

Keep an eye on your bank, email, and other accounts for unusual activity after an incident.

Contact Relevant Organisations

Notify your bank, service providers, or support agencies so they can help secure your accounts and limit damage.

Seek Support

Reach out to support services or trusted people for advice, guidance, and emotional support during recovery.

CONTINUE

Check Your Understanding

Test your knowledge with the following questions. Answering them will help you remember the key points about reporting and recovering from cyber incidents—and prepare you to act if something goes wrong.

Why is it important to report a cyber incident as soon as possible?

- It increases the chance of recovering and helps protect others.

- It's only necessary if you lose money.
- Reporting is optional and rarely helps.
- You should wait to see if the problem goes away.

SUBMIT

What should you do when reporting a scam or cyber incident?

- Provide as much detail as possible, including evidence and contact information.
- Only give your name and phone number.
- Wait for someone to contact you first.
- Just tell a friend and hope for the best.

SUBMIT

What is a good first step after experiencing a cyber incident?

- Change your passwords and monitor your accounts.
- Ignore the incident and move on.
- Delete your accounts immediately.
- Wait to see if anything else happens.

SUBMIT

CONTINUE

Course Summary and Next Steps.

Congratulations on completing this course! You've learned how to prevent, recognise, and respond to cyber threats, and how to support others in your community. Remember, cyber safety is an ongoing journey—keep your knowledge up to date, stay alert, and continue sharing what you've learned to help make the online world safer for everyone.

Every action you take helps make Australia a safer place online—stay alert, stay informed, and help others do the same.