CYBER WARDENS **FOUNDATIONS**

The Cyber Wardens Foundations course is designed for time-challenged small business owners and employees. It provides essential cyber security awareness skills to help protect your business and start important conversations about cyber safety with your team, customers, and suppliers.

This module covers:

- *Seven common cyber security red flags*
- *The top three cyber crimes targeting small businesses*

You will learn how to:

- *Recognise warning signs that your business may be targeted by cyber threats*
- *Build safer digital habits across your business operations*
- *Minimise the risk of cyber attacks and scams*

Why Cyber Security Matters for Small Businesses

Small businesses are increasingly targeted by cyber criminals because they often lack the defences of larger organisations.

A single breach can lead to stolen data, financial loss, reputational damage, and long-term disruption. Cyber security is no longer optional — it's a necessary part of doing business safely in the digital age.

CyberWardens.

Lesson 01

Seven Cyber Security Red Flags

Knowing what scams to look out for — and how to respond to them — is one of the most effective ways to protect your business. Below are seven common red flags that may signal a cyber attack or scam attempt.

"If I had done this course years ago, I probably never would have been hacked."

– Small Business Owner

Cyber scams can appear not only through emails but also via SMS, social media messages, and website forms. Stay vigilant across all communication channels.

1. Unexpected invoices

Scammers may send fake invoices during busy times like end-of-month or end-of-financial-year, hoping they'll be processed without close review.

2. Uncommon or misspelt email addresses

Be alert to small errors in email addresses that mimic legitimate businesses. One misplaced letter can mean the sender isn't who they claim to be.

3. Change of banking details

If a supplier suddenly asks you to send payment to a different bank account, treat this as a major warning sign. Always confirm changes using a trusted contact method — never rely on phone numbers or email addresses provided in the suspicious message.

4. Pressure to act urgently or confidentially

Scammers create panic or secrecy to rush you into action. Be wary of requests that demand immediate action or discourage you from discussing with others.

5. Unusual requests

If someone you know asks for something out of character — such as gift cards, passwords, or urgent transfers — double check before taking action.

6. Unusual or hidden links

Look closely at web links before clicking. Fraudulent links may look legitimate at a glance but contain typos or redirect to fake websites.

7. Suspicious attachments

Files that don't match their labels — such as a file named "photo" that turns out to be a .zip or .rar file — are a red flag. Avoid downloading or opening anything that seems even slightly off.

CyberWardens.

Lesson 02

The Top Three Cyber Crimes Affecting Small Businesses

> ***"Cyber security knowledge is like insurance — you hope you never need it, but you're glad you have it."***
>
> ***– Small Business Owner***

Cyber criminals are constantly evolving their tactics. According to national threat reports, the most common cyber crimes affecting small businesses are:

1. Inbox Break-ins (Business Email Compromise - BEC)

Cyber criminals may gain access to a business email account and use it to impersonate staff or suppliers. These scams often involve:

- ***Invoice fraud*** *– sending fake payment requests*
- ***Employee impersonation*** *– posing as someone from within your business*
- ***Company impersonation*** *– mimicking an external supplier*

Look out for:

- *Unusual or unfamiliar email addresses*
- *Unexpected invoice or payment requests*
- *Urgent or secretive instructions*

Always verify financial changes using independent, trusted communication channels.

2. Uncommon or misspelt email addresses

Phishing attacks trick you into sharing sensitive information such as login credentials or payment details. These can occur through:

- *Email*
- *Phone calls (also called "vishing")*
- *SMS messages (known as "smishing")*

Be cautious of unsolicited requests for logins, PINs, or account information — especially if they create urgency or emotional pressure.

3. Banking Burglary

Online banking scams allow cyber criminals to access your accounts and move funds without your permission.

To protect your business:

- *Use unique, strong passwords or passphrases for each banking account*
- *Ensure passwords are at least 14 characters long and include a mix of letters, numbers, and symbols*
- *Avoid using the same password across systems*

Use multi-factor authentication whenever possible

Wrapping Up

Congratulations — you've completed the Cyber Wardens Foundations module!

You've now learned how to:

- *Identify seven common red flags for cyber threats*
- *Understand the most frequent types of cyber crimes*
- *Take the first steps in protecting your business from online attacks*

Next, you can deepen your knowledge by completing the **Cyber Wardens Level One** course, which covers:

- *Protecting your most important business information*
- *Defending against more complex scams and digital break-ins*
- *Encouraging cyber safety across your team and wider network*

CYBER WARDENS **LEVEL ONE**

Welcome to Cyber Wardens Level One training.

This course is designed for small business owners and staff who want to better understand and defend against common cyber threats. It provides basic but essential cyber security measures you can take to protect your systems, your customers, and your business reputation.

Cyber security doesn't need to be complex. The following modules focus on practical actions — no jargon, no fluff — just clear steps that anyone can follow.

Course Objectives

This course is divided into four modules. After completing all four, you'll be able to:

- *Spot common tricks and scams*
- *Promote cyber safety in your team*
- *Prevent digital break-ins*
- *Protect and preserve business and customer data*

Module Overview

Module **01**	**Cyber Threats**	*Understand how and why cyber criminals target small businesses, and learn to identify the most common forms of attack.*
Module **02**	**Cyber Wardens Mindset**	*Learn how everyone in your team plays a role in cyber safety — and how to embed the right mindset.*
Module **03**	**Cyber Wardens Skillset**	*Gain foundational skills for identifying threats, safeguarding your data, and responding to breaches.*
Module **04**	**Cyber Wardens Toolkit**	*Use practical tools and checklists to strengthen your cyber defences, including updates, backups, and password security.*

Why are small businesses at risk?

Many small business owners think they're too small to be targeted. But in reality:

- *Cyber criminals prefer smaller targets with weaker defences*
- *Many small businesses lack the time or expertise to implement safeguards*
- *Human error remains the most common vulnerability*

Key Statistics

- *44% of small business owners and staff have experien ced a cyber attack*
- *51% believe an attack is inevitable*
- *Only 21% feel confident responding to an attack*
- *95% of attacks start with human error*
- *$46,000 is the current average cost of an attack*
- *A cyber attack is reported every 6 minutes in Australia*

Common Misconceptions

☒ "My business is too small to be a target."

False. Cyber criminals use automated tools to scan and attack thousands of systems at once.

☒ "You need to be tech-savvy to be safe."

False. Most attacks rely on psychological tricks, not technology failures.

☒ "We've never had a breach, so we must be secure."

False. Many breaches go undetected or unreported — and it only takes one mistake.

Top 3 Cyber Threats to Small Business

1. Inbox Break-ins (Business Email Compromise)

Criminals gain access to your business email account and impersonate you or your staff. They may:

- *Redirect payments*
- *Send fake invoices*
- *Request confidential information*

2. Fake Invoices and Payment Redirection Scams

Scammers send invoices that appear to come from trusted suppliers but contain altered payment details.

3. Online Banking Fraud

Once they gain access to your login credentials, cyber criminals can empty your accounts or make unauthorised transactions.

Understanding Phishing

Phishing is one of the most common tactics used by cyber criminals. It involves tricking you into revealing sensitive information or downloading malicious files.

Warning Signs of Phishing Messages

- *Unusual or misspelt sender email addresses*
- *Urgent or threatening language (e.g. "Your account will be locked!")*
- *Generic greetings like "Dear Customer"*
- *Poor grammar or formatting*
- *Suspicious links or unexpected attachments*
- *Requests to confirm personal or financial details*

Phishing attempts can arrive via email, SMS, phone calls, or even social media messages.

Business Email Compromise (BEC) Scams

A BEC scam is when a criminal impersonates someone in your business (e.g. a manager or supplier) to request:

- *Urgent payments*
- *Gift card purchases*
- *Sensitive information*

These scams work because they appear familiar and are often timed when people are busy, distracted, or under pressure.

How to Spot a BEC Scam

Ask yourself:

- *Is the sender's email address unusual or slightly different?*
- *Is this request out of the ordinary?*
- *Does it include urgency or secrecy?*
- *Are there signs of poor grammar or formatting?*

If anything feels off, confirm the request using a trusted method — not by replying to the email or using the contact details provided in the message.

Quick Checklist: Is It a Scam?

If you receive an email request at work, consider:

- *Is the email from a recognised address?*
- *Is the request expected and appropriate?*
- *Are the payment details unchanged?*
- *Is the language professional and accurate?*

If you answer "no" to any of the above, stop and verify before acting.

The Role of People in Cyber Security

Technology can only go so far. Most successful attacks don't exploit software — they exploit people.

That's why awareness training and good habits are essential. Cyber criminals rely on people being rushed, tired, or untrained. The more prepared your team is, the more resilient your business becomes.

Reflections Activity

Reflection Prompt 1:

What would happen if your business experienced a cyber attack tomorrow? List the potential consequences in your notes and consider how it would impact:

- *Daily operations*
- *Customer trust*
- *Financial stability*
- *Your personal wellbeing*

You can complete this reflection now or revisit it after finishing the course.

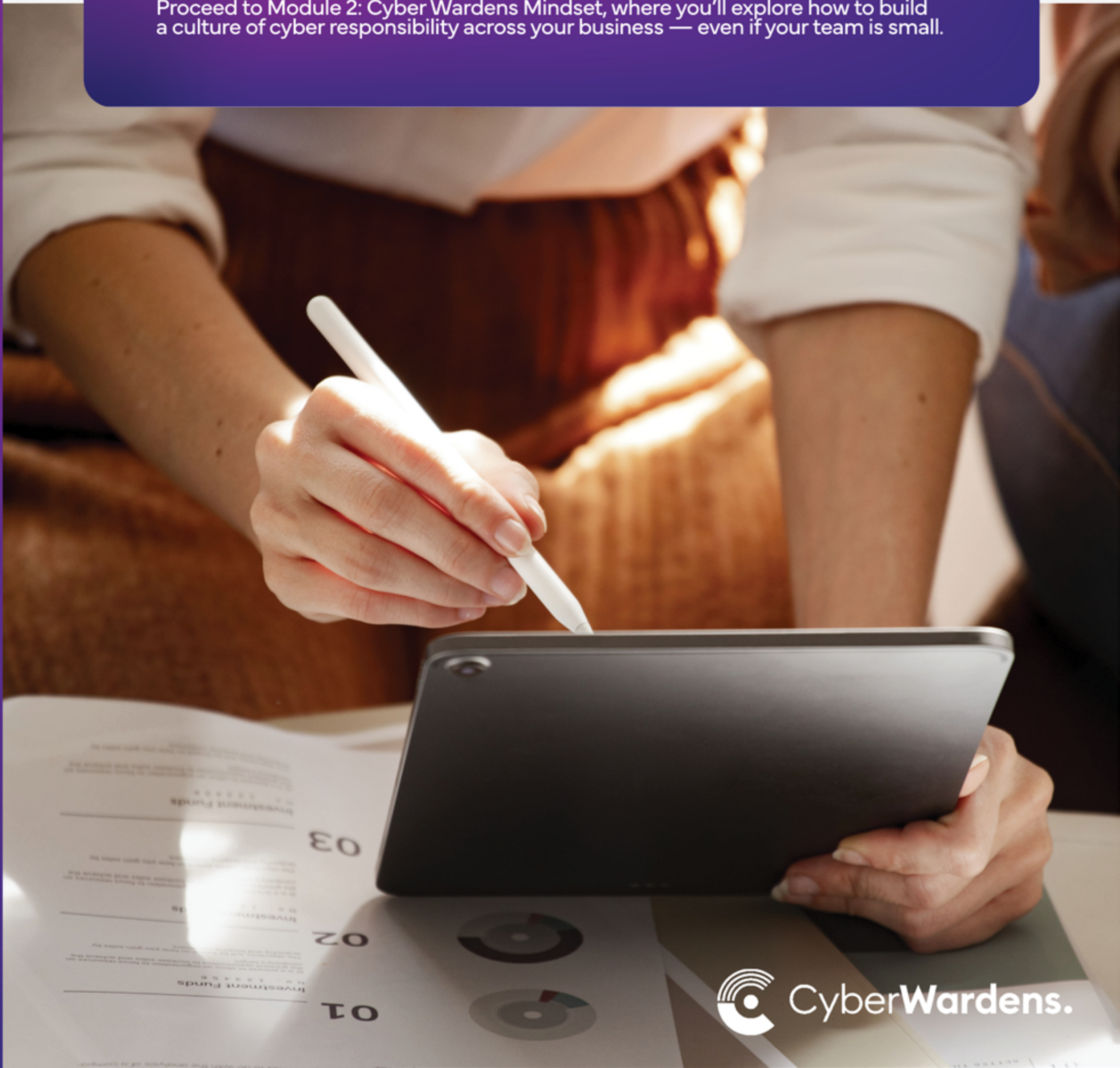
Summary of Module 1

In this module, you've learned:

- *Why small businesses are frequent targets*
- *The three most common cyber threats*
- *How to identify phishing and BEC scams*
- *The importance of awareness and staff training*
- *That human error is the most common gateway for attacks*

Next Steps

Proceed to Module 2: Cyber Wardens Mindset, where you'll explore how to build a culture of cyber responsibility across your business — even if your team is small.



Module 02 | Cyber Wardens Mindset

Like fire wardens or first aid officers, Cyber Wardens take on a shared responsibility for safety — but in the digital space.

Your Role:

- *Promote cyber safety habits in your business*
- *Champion regular training and reminders*
- *Lead by example with strong practices*

Biggest Threat: People, Not Technology

95% of cyber attacks happen due to human error. Scammers:

- *Exploit distraction, busyness, and untrained staff*
- *Trick employees through fake emails and social engineering*

Top 5 People-Based Vulnerabilities:

1. Lack of training

2. Human error

3. Working offsite

4. Busy teams missing details

5. Hackers targeting individuals personally

Reflection Activity:

Create a plan for how you will promote cyber safety in your business — alone or with your team.

Your business runs on data — and criminals want it.

What needs protection?

- *Communication channels: Email, socials, marketing systems*
- *Inventory and orders: Sales data, customer info*
- *Financial systems: Online banking, payment platforms*
- *Websites: Contact forms, reviews, support records*

Criminals Use Data To:

- *Create fake invoices*
- *Impersonate your brand online*
- *Steal identities or sell data to competitors*

What To Do If You're Breached

*1. **Notify your bank** immediately*

*2. **Stop all contact** with the scammer*

*3. **Protect other accounts** (change passwords, enable MFA)*

*4. **Report the incident** (ScamWatch, ACSC)*

*5. **Get help** (IDCARE or a cyber specialist)*

Reflection Activity:

Map out all the business data you hold. Where is it stored? How is it protected?

Module 04 | Cyber Wardens Toolkit

Cyber protection starts with four essential tools.

Tool #1: Automatic Updates

- *Turn on auto-updates for operating systems, apps, plugins, and antivirus software*
- *Don't forget: websites, payment systems, and team devices*

Bonus Tips:

- *Unused software can pose risks — uninstall what you don't use*
- *Don't delay updates — snoozing creates vulnerabilities*

Reflection Activity:

Complete the "Automatic Updates Register".

Tool #2: Multi-Factor Authentication (MFA)

- *MFA adds an extra security layer beyond passwords*
- *Use it on: email, banking, payment accounts, socials, admin platforms*

Types of MFA:

- *SMS codes (least secure)*
- *Authenticator apps (recommended)*
- *Biometrics (face/fingerprint recognition)*

Reflection Activity:

List your key accounts. Schedule time to enable MFA on all of them.

Tool #3: Passwords & Passphrases

- *Use long, strong, and unique passwords Avoid reusing passwords — each account and team member should have their own login*
- *Upgrade to passphrases: Random, unrelated words (e.g. BananaPencilMonstera!)*

Credential Stuffing Alert:

Reused passwords allow criminals to access multiple systems if one breach occurs.

Reflection Activity:

Review your current passwords. Replace weak ones or start using a password manager.

Tool #4: Backup & Recovery

- *Keep secure backups — both physical (external drives) and cloud-based*
- *Test your ability to restore data monthly*

Best Practices:

- *Store at least one backup offsite*
- *Secure your cloud backups with MFA and strong passphrases*
- *Ensure all data is uploaded — local files aren't automatically protected*

Reflection Activity:

Create a clear backup process and share it with your team.

FINAL RECAP: YOU'RE A CYBER WARDEN!

You've now learned how to:

- *Understand the biggest cyber risks to your business*
- *Build a cyber-aware culture*
- *Identify and protect valuable data*
- *Use key tools to lock digital doors*

Stay vigilant, keep training your team, and check for updates from trusted sources like **the Australian Cyber Security Centre (ACSC) and Scamwatch.**

CYBER WARDENS LEVEL TWO

Module 01 | AI in Your Business Life

"I own my own naturopathy practice and we love using technology to get the best results for our clients. It wasn't until I received a convincing fake email from a long-term client saying they were sick and needed money for their treatment that I realised I needed to talk to my staff about being aware of AI scams."

– Small business owner

About This Lesson

Artificial Intelligence (AI) is designed to mimic human thinking — it learns from data, recognises patterns, and makes decisions. It already shapes how we live and work, often without us even noticing.

In this lesson, you will learn:

- *How AI can help you save time and strengthen your business*
- *Where cyber criminals are using AI to steal information and money*
- *Why it's important to understand AI risks within your business and industry*

How AI Supports Business

AI is often invisible but working constantly in the background to:

- *Filter scam emails from your inbox*
- *Manage your calendar*
- *Help you find the best prices*
- *Automate customer service*
- *Improve fraud detection*
- *Transcribe meetings and notes*
- *Recommend marketing strategies*
- *Assist with hiring and scheduling*
- *Support financial security*
- *Strengthen password protection*

AI Is a Tool — It's How It's Used That Matters

Cyber criminals are also using AI to:

- *Generate realistic phishing emails that appear to come from clients or suppliers*
- *Create deepfake videos or voice messages to impersonate trusted people*
- *Launch automated attacks that crack passwords or exploit vulnerabilities faster than humans*

Summary: What You've Learned

- *AI is embedded in many business tools — it helps save time and boost productivity*
- *Criminals use AI to create more convincing, faster, and more dangerous scams*
- *Understanding how AI works is key to using it safely*
- *Small businesses should embrace AI, but stay alert to AI-powered cyber threats*

Module 02 | AI Threats and Scams

> *"I run a small accounting firm and last month I almost fell for an AI-generated scam. I got an email that looked exactly like it was from the government. It even had my business name and mentioned an outstanding tax obligation. It was so well-written — no typos, no weird formatting — just professional and urgent."*
>
> *– Small business owner*

About This Lesson

AI has supercharged cyber scams, making them more personalised and believable. This module covers the most common AI-powered threats and how to stay safe.

You will learn about:

- *AI-powered phishing and business email compromise (BEC)*
- *Deepfake and impersonation scams*
- *Session hijacking*
- *Fake AI chatbots and malicious tools*

▸ AI-Powered Phishing and Business Email Compromise (BEC)

Phishing scams now look and sound like trusted individuals or organisations. AI makes it easy to imitate writing style, tone, and branding.

How to stay safe:

- *Always verify unusual requests using official contact details*
- *Look closely at email addresses — small changes may signal spoofing*
- *Use multi-factor authentication (MFA) for all accounts*

▸ Deepfake and Impersonation Scams

AI-generated video and voice can now imitate clients, colleagues, or managers.

Common deepfake scam scenarios:

- *A fake video call from a boss asking for urgent transfers*
- *An AI-generated voicemail approving a fake invoice*
- *A fake chatbot posing as a customer service rep*

How to stay safe:

- *Train your team to spot deepfakes (unnatural voice tone, strange pauses, lip sync issues)*
- *Create internal code words for sensitive requests*
- *Always verify changes to payments or authorisations with a phone call*

▸ Session Hijacking

A "session" refers to your logged-in state when using online accounts. AI can help attackers steal session tokens and act on your behalf.

How to stay safe:

- *Always use secure websites (look for HTTPS)*
- *Avoid logging into sensitive accounts using public Wi-Fi*
- *Close all active sessions when done*

▸ Fake AI Chatbots and Malicious AI Tools

Cybercriminals may insert fake AI chatbots on scam websites or disguise malicious software as AI "business tools."

How to stay safe:

- *Only use chatbots from trusted providers*
- *Monitor chatbot behaviour and train your team to identify red flags*
- *Never share sensitive business data with unverified AI platforms*

Basic Rules for AI Safety

- *Never input customer or financial data into unknown AI platforms*
- *Always verify unexpected requests or alerts*
- *Keep all software and systems updated*
- *Train staff on new risks and verification steps*

Summary: What You've Learned

- *AI scams include phishing, deepfakes, session hijacking, and fake tools*
- *Cyber criminals use AI to remove the usual "red flags"*
- *Good habits — like verifying requests and using MFA — offer strong protection*
- *Awareness and training are the best defences against advanced scams*

CYBER WARDENS **REFRESH**

Welcome to Cyber Wardens Refresh

This self-paced course refreshes your skills and knowledge from Cyber Wardens Foundations and Level One. It introduces new and emerging cyber threats facing small businesses.
You'll learn how to:

- *Identify top attacks and scams targeting small businesses*
- *Promote cyber safety in your workplace*
- *Protect valuable business information (data)*
- *Use four core tools: automatic updates, multi-factor authentication, passwords/passphrases, and data backup*

CyberWardens.

Module **01** **Cyber Threats**

Module 01 | Cyber Threats

You'll refresh your knowledge of phishing attacks and Business Email Compromise (BEC) scams, and be introduced to emerging cyber threats including:

- *Artificial Intelligence (AI) misuse*
- *Session hijacking*
- *Quishing (QR code phishing)*

Reflection Activity 1.1 – Cyber Security Breach
Consider the consequences of a cyber security breach to your business. List these in your Reflections notebook.

Phishing
Phishing is when cyber criminals impersonate a trusted person or business to steal sensitive information.

Reflection Activity 1.2 – Phishing Attack
Do you know of any businesses affected by phishing? What was the impact? How can your team be trained to identify phishing attempts?

Business Email Compromise (BEC)
The three main BEC scams are:

- *Invoice fraud*
- *Employee impersonation*
- *Company impersonation*

Reflection Activity 1.3 – Inbox Break-ins
List the measures you can take to protect your business and staff from BEC scams.

Emerging Threats Overview

- ***AI misuse*** *– Cyber criminals can now use AI to craft more believable scams*
- ***Session hijacking*** *– Criminals intercept your web sessions to steal access*
- ***Quishing*** *– Malicious QR codes that direct users to fraudulent sites*

Module 02 | Cyber Wardens Mindset

Module 02 | Cyber Wardens Mindset

This module helps you build a mindset for cyber safety and confidently lead conversations within your team.

You'll cover:

- *How to create a cyber-safe culture*
- *Five important cyber safety habits*
- *Managing out-of-office email messages*

Reflection Activity 2.1 – Promoting Cyber Safety
Create a plan to keep cyber safety a priority in your business. Use the templates in your Reflections notebook.

Five Important Cyber Safety Habits

Do you know of any businesses affected by phishing? What was the impact? How can your team be trained to identify phishing attempts?

- ***Shut Down Devices*** *– Avoid leaving devices in sleep mode.*
- ***Use Passphrases & Password Managers*** *– Strengthen access with secure logins.*
- ***Report Suspicious Emails*** *– Alert Scamwatch or the impersonated business.*
- ***Use Unique Logins*** *– Don't share credentials between team members.*
- ***Turn on Automatic Updates*** *– Apply system and software updates promptly.*

Spotlight: Out-of-Office Messages

Avoid sharing travel plans or personal details in automated replies. Use general contacts where possible.

Example:

Thank you for your email. I'm currently away and may be delayed in responding. For urgent matters, please contact [team email] or call our office at [number].

Module **03** | **Cyber Wardens Skillset**

Module **03** | **Cyber Wardens Skillset**

This module builds your response plan if a digital break-in occurs. You'll also learn key soft skills and device security basics.

Five Steps After a Breach

1. Notify Your Bank

2. Stop Contact with the Scammer

3. Protect Other Accounts

4.Report the Attack (to Scamwatch or ACSC)

5.Get Help (e.g. IDCARE)

Reflection Activity 3.1 – Where is your data?
List all data your business generates and where it's stored. Work with your team to identify any gaps.

Soft Skills You Need

List all data your business generates and where it's stored. Work with your team to identify any gaps.

- ***Calm communication***
- ***Decision-making under pressure***
- ***Team coordination***
- ***Accountability***

Physical Security

Lock devices when unattended, avoid shared devices without password protection, and use secure storage for backups.

Module 04 | Cyber Wardens Toolkit

Module 04 Cyber Wardens Toolkit

You'll revisit practical tools to defend your business and recover from attacks.

Tool 1: Automatic Updates

Audit your devices. Ensure updates are active for:

- *Operating systems*
- *Apps, browsers, and plug-ins*
- *Payment systems and smart devices*
- *Website platforms and plug-ins*
- *Antivirus software*

Reflection Activity 4.1 – Update Register

List devices that need updates. Schedule monthly reminders for your team.

Tool 2: Multi-Factor Authentication (MFA)

Add MFA to critical accounts (banking, email, social media). This is your virtual alarm system.

- *Calm communication*
- *Decision-making under pressure*
- *Team coordination*
- *Accountability*

Reflection Activity 4.2 – MFA Planning

Create a list of business-critical platforms and schedule a session to enable MFA on all.

Tool 3: Strong Passwords & Passphrases

Use:

- *14+ character passwords with symbols and numbers*
- *Passphrases that are memorable and unpredictable (e.g. SingBananaPencilMonstera)*
- *Password managers for storage*

Reflection Activity 4.3 – Password Audit

Review current passwords and set a timeline to switch to stronger ones or passphrases.

Tool 4: Backup & Recovery

Use both:

- *External hard drives (kept offsite and swapped regularly)*
- *Cloud storage with encryption and automatic backups*
- *Test your data recovery process monthly.*

Reflection Activity 4.4 – Backup Planning

Define your team's backup schedule and storage methods. Practice recovery steps regularly.

Additional Tools

- Wi-Fi Passwords – Use strong, unique Wi-Fi passwords and manage guest access
- Password Managers – Use a trusted tool to manage and share passwords securely

CyberWardens.

CYBER WARDENS **REFRESH**

Congratulations, you've completed Cyber Wardens Foundations.

Thank-you for helping making Australia more cyber secure.
To verify you've read the material and to receive your certificate, please tick this box.

CyberWardens.