

Cyber Wardens Champions Guide

Your toolkit for leading
the way in small business
cyber security



Welcome to the Cyber Wardens Champions Program

This guide is designed to equip you with the knowledge, practical tools, and confidence to promote the Cyber Wardens program in your workplace, industry, or community. As a Champion, you'll play a vital role in helping others become more cyber aware, build safer digital habits, and protect their businesses from everyday cyber threats.

What you'll learn:



Your critical role as a Cyber Wardens Champion

How to drive cyber security culture change



Effective ways to communicate about cyber threats

Practical strategies to engage different audiences



Tools and resources to support your champion efforts

Let's begin your journey to becoming an effective cyber security advocate!



Module 1: Your role as a Cyber Wardens Champion

In this module, you'll learn what it means to be a Cyber Wardens Champion and how to use your influence to promote cyber safety in your workplace or community. You'll understand the difference between informal and formal approaches to engagement and identify how your unique role can help protect others from cyber threats. By the end, you'll be equipped to lead by example and support others in building safer digital habits.

What is a Cyber Wardens Champion?

A Cyber Wardens Champion educates and motivates others to take simple steps to improve their cyber security at work and at home. Champions operate in two key ways:

Informal approach: Through casual, everyday conversations

Formal approach: By organising group training, workshops and skills development in workplaces, networks or professional groups

Key insight:

Being a Cyber Wardens Champion isn't about being an expert—it's about using your connections, care, and influence to build a safer, more secure community.

Who should become a Cyber Wardens Champion?

You don't need special education or qualifications to become a Cyber Wardens Champion. All you need is an interest in learning how to help others protect themselves against cyber threats.

Ideal candidates include:

- ✔ Small business owners, managers or employees
- ✔ Advisors who work with small businesses (accountants, bookkeepers, financial advisors)
- ✔ Community group members, volunteers in not-for-profit networks
- ✔ HR professionals who onboard and train personnel
- ✔ IT providers who need simplified ways to talk to clients
- ✔ Individuals who care about the cyber security of people around them

Why your role matters

As a Cyber Wardens Champion, your everyday role already positions you to make a difference. Whether you're a connector, advisor, role model, or protector, recognising your strengths will help you spread cyber safety more effectively.

Your role, your impact:

- ✔ **Natural connector:** Your work, community, and social networks give you the opportunity to spread cyber safety
- ✔ **Cyber safety role model:** Lead by example and encourage others to take Cyber Wardens courses
- ✔ **Small business influencer:** Boost awareness and protect businesses from online threats
- ✔ **Trusted advisor:** Add cyber safety tips to the guidance you already provide
- ✔ **Community champion:** Help protect sensitive information in community organisations
- ✔ **Onboarding hero:** Guide new staff with simple, easy-to-understand cyber safety practices
- ✔ **Tech translator:** Break down cyber security into simple language
- ✔ **Everyday protector:** Help protect family, friends, and neighbours from cyber risks

Benefits of becoming a champion

Becoming a Cyber Wardens Champion offers personal and professional growth:

- ✔ **Better communications skills:** Learn to explain cyber risks in simple, accessible language
- ✔ **Enhanced cyber awareness:** Gain deeper understanding of cyber threats affecting small businesses
- ✔ **Stakeholder knowledge:** Identify all parties who impact business security
- ✔ **Leadership development:** Demonstrate leadership by coordinating training
- ✔ **Boosted confidence:** Feel empowered to take charge of cyber safety
- ✔ **Career edge:** Add valuable skills to your professional toolkit





Module 2: Cyber security as a team sport

In this module, you'll discover how cyber security involves a wide network of people, not just IT staff. You'll map your own "cyber team" and learn how everyday actions can strengthen or weaken your collective defences. By the end, you'll understand how to build a stronger cyber safety culture in your business or community.

Understanding your cyber security team

When it comes to cyber security, your "team" extends far beyond just your immediate colleagues. Let's map who's on your team:

The helpers

- ✓ Family members
- ✓ Friends
- ✓ Community groups
- ✓ Business networks
- ✓ Peer groups

The game changers

- ✓ Business owners
- ✓ Key employees
- ✓ IT support providers
- ✓ Suppliers and vendors
- ✓ Professional and regulatory bodies

The guests

- ✓ General customers
- ✓ Website visitors
- ✓ Local community members

The sharers

- ✓ Social media influencers
- ✓ Community leaders
- ✓ Industry bloggers
- ✓ Business associations

Activity: Create your personal "Cyber Team Map" by listing specific people and organisations in each category.

The urgency of cyber safety culture

Recent research highlights why building a culture of cyber safety is critically important:

2024 Small Business Survey findings

- ✓ Cyber security is the third largest threat (54%) to small businesses
- ✓ 51% of small business owners believe cyber security is too complicated to implement
- ✓ 51% allow family members to use work devices
- ✓ 50% use public Wi-Fi without a VPN
- ✓ 50% share personal information on social media
- ✓ 68% of employees use personal devices for work
- ✓ 53% share passwords with colleagues

2025 Cyber Security Pulse Check AI-related concerns:

- ✓ 78% believe cyber criminals are becoming more sophisticated due to AI
- ✓ 74% think rapidly advancing technology poses a risk to their business
- ✓ 56% are concerned about AI and automation risks to cyber security
- ✓ Only 41% feel confident their business is protected from emerging threats
- ✓ 37% feel unprepared to protect against AI-driven cyber threats

Key insight: With 95% of attacks targeting people rather than systems, and the average cost of an attack rising to \$56,600, building a culture of cyber awareness has never been more crucial.

Real-life team example – Casey’s story

Real-life case studies make cyber threats more relatable and easier to understand. They help people spot warning signs, learn from others’ experiences, and feel less alone if they’ve been affected. Here’s an example illustrating how to put together your “cyber team”.

Case study: Casey at the medical centre

Casey works part-time at the front desk of a local medical centre where he:

- ✓ Answers phones
- ✓ Checks patients in/out
- ✓ Collects payments
- ✓ Updates records
- ✓ Manages appointments
- ✓ Provides information to patients

Casey is also studying personal training at TAFE, plays soccer, and dreams of running his own gym.

Helpers

- ✓ His mother (who runs a personal trainer business and pays him as a contractor)
- ✓ His partner (with whom he shares a bank account)
- ✓ His local soccer club

Persons of influence

- ✓ Medical centre owners
- ✓ Doctors and healthcare providers
- ✓ Medical centre IT support
- ✓ Patient record software vendors
- ✓ Healthcare regulatory authorities

Guests

- ✓ Patients
- ✓ Website visitors
- ✓ Local community members

Sharers

- ✓ Local health influencers
- ✓ Community healthcare forums
- ✓ Medical industry associations

Discussion: What cyber risks might Casey face in his various roles? How could these risks impact the different members of his cyber team?



Module 3: Communicating about cyber security

In this module, you'll learn how to recognise and overcome common barriers that prevent people from engaging with cyber security, such as confusion, apathy, or habits. You'll explore how to use simple language, relatable analogies, and the right tone to make your message clear and motivating. By the end, you'll be able to craft effective, audience-specific messages that inspire action and build a culture of security.

Understanding communication barriers

Effective cyber security communication requires recognising and overcoming common barriers:

Behavioural barriers

- ✓ Convenience prioritised over security
- ✓ Resistance to changing habits
- ✓ Security fatigue from too many passwords/procedures
- ✓ Time constraints for implementing security measures

Attitudinal barriers

- ✓ "It won't happen to me" mindset
- ✓ Belief that cyber security is solely IT's responsibility
- ✓ Perception that protection requires technical expertise
- ✓ Feeling overwhelmed by complexity

Knowledge barriers

- ✓ Technical terminology confusion
- ✓ Misconceptions about who is targeted
- ✓ Lack of awareness about threats
- ✓ Uncertainty about protective measures

Effective language and tone

How you communicate about cyber security can significantly impact engagement:

Language best practices:

- ✓ Use everyday analogies (e.g., "You lock your front door every day, so why not lock your digital door?")
- ✓ Focus on simple, actionable steps
- ✓ Avoid technical jargon when explaining concepts
- ✓ Make content relevant to daily life
- ✓ Be inclusive and avoid language that might alienate any groups

Tone considerations:

- ✔ Be encouraging Recognise efforts and progress
- ✔ Believe in people's ability to improve
- ✔ Be conversational and approachable
- ✔ Show empathy for the challenges people face

Example transformations:

Instead of saying...	Try saying...
"Your weak password puts the entire company at risk"	"Strong passwords are like sturdy locks - they keep your valuable information safe"
"Phishing attacks exploit human vulnerability"	"Scammers send deceptive emails hoping you'll click without thinking - taking a moment to check can protect you"
"Multi-factor authentication deployment is mandatory"	"Adding a second verification step is like having both a key and an alarm code - double protection for what matters"
"Security protocols must be adhered to"	"Following our simple security steps helps protect everyone on the team"

Crafting your message

When preparing to talk about cyber security, consider these message-crafting strategies:

Know your audience

- ✔ What's their existing knowledge?
- ✔ What do they care about protecting?
- ✔ What are their primary concerns or pain points?
- ✔ What motivates them?

Personalise the message

- ✔ Connect cyber security to their specific role
- ✔ Highlight potential personal impacts
- ✔ Relate to their industry or business
- ✔ Address their specific concerns

Structure your message

- 1. Hook:** Start with an engaging fact, story or question
- 2. Why:** Explain why this matters to them specifically
- 3. What:** Present the key concept
- 4. How:** Provide simple steps
- 5. Benefit:** Emphasise the positive outcomes of taking action

Practice scenario: Imagine you need to talk to a small retail shop owner about using strong passwords. Craft a brief message following the structure above.



Module 4: Engaging your audience

In this module, you'll learn how to spot opportunities to talk about cyber security across workplaces, communities, and professional networks. You'll explore strategies for tailoring your message to various audiences, including small business owners, seniors, and young adults, using relatable and engaging approaches. By the end, you'll be equipped to deliver impactful learning experiences that make cyber safety practical, relevant, and easy to apply.

Identifying engagement opportunities

As a Cyber Wardens Champion, you can find opportunities to engage different audiences:

For small business teams

- ✓ Team meetings
- ✓ Onboarding sessions
- ✓ Lunch and learn events
- ✓ Internal newsletters
- ✓ Training days
- ✓ Company chat platforms

For community groups

- ✓ Club meetings
- ✓ Community events
- ✓ Newsletters
- ✓ Social gatherings
- ✓ Volunteer orientation
- ✓ Fundraising events

For clients and customers

- ✓ One-on-one consultations
- ✓ Client education sessions
- ✓ Welcome packets
- ✓ Follow-up communications
- ✓ Website resources
- ✓ Social media content

For professional networks

- ✓ Industry events
- ✓ Professional development sessions
- ✓ Association meetings
- ✓ Online forums
- ✓ Networking events
- ✓ Conferences

Engagement strategies for different groups

Different groups respond to different approaches. Consider these tailored strategies:

For non-technical individuals

- ✓ Focus on real-life examples
- ✓ Use simple analogies (e.g. comparing passwords to keys)
- ✓ Provide visual guides and checklists
- ✓ Emphasise personal impact (protecting photos, banking, etc.)

For business owners

- ✓ Highlight potential financial and reputational costs
- ✓ Discuss protection of client data
- ✓ Connect security to business security
- ✓ Focus on simple solutions that don't require extensive resources

For employees

- ✓ Relate security to job protection
- ✓ Discuss role-specific responsibilities
- ✓ Make security part of daily routines
- ✓ Reward good security practices

Creating engaging learning experiences

When organising formal training or workshops, consider these best practices:

Interactive elements

- ✓ Scenario-based discussions
- ✓ Security quizzes with prizes
- ✓ Role-playing common scam situations
- ✓ Hands-on practice with tools

Visual content

- ✓ Short, engaging videos
- ✓ Infographics summarising key points
- ✓ Before/after demonstrations
- ✓ Visual comparisons (e.g., weak vs. strong password)

Personalised learning

- ✓ Allow participants to bring real questions
- ✓ Provide individual feedback on security practices
- ✓ Create customised checklists for different roles
- ✓ Offer follow-up support for specific concerns

Experiential learning

- ✓ Simulate phishing emails (with safe examples)
- ✓ Do security checks together
- ✓ Practice creating strong passwords
- ✓ Demonstrate real security tools in action

Key insight: People learn best when they can connect new information to their existing knowledge and when they can immediately apply what they've learned.



Module 5: Practical resources and tools

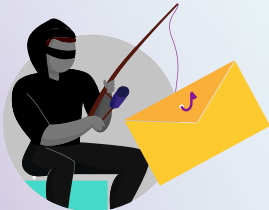
In this module, you'll explore real-world scenarios that demonstrate common cyber threats like phishing, fake invoices, and phone scams. You'll learn to identify warning signs, respond safely, and guide others through practical steps to protect themselves. By the end, you'll be able to use stories and quick-reference tools to build cyber awareness and confidence in your workplace or community.

Cyber Wardens scenarios

Use these scenarios to help illustrate common cyber threats and appropriate responses:

Scenario 1: Phishing email

Maria received an email that appeared to be from her bank, stating there was a problem with her account and requesting she click a link to verify her details. The email addressed her by name and included the bank's logo, but the sender's email address was slightly different from the bank's usual address. The link directed her to a page that looked like her bank's website but had a slightly different URL.



Discussion questions:

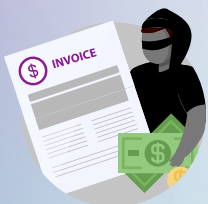
What are the red flags in this scenario?

What should Maria do instead of clicking the link?

How could this affect Maria personally and professionally?

Scenario 2: Fake invoice

Alex, a small business owner, received an invoice for office supplies from what appeared to be their regular supplier. The invoice looked legitimate with the supplier's logo and contained details of previous orders. However, the bank account number for payment was different from the one they normally use, and the email requested urgent payment within 24 hours to avoid late fees.



Discussion questions:

What are the warning signs in this scenario?

What steps should Alex take before making any payment?

How might this scam impact Alex's business?

Scenario 3: Banking burglary

Sam received a phone call from someone claiming to be from his bank's security team. The caller knew Sam's name, address, and the last four digits of his credit card. They said they had detected suspicious activity on his account and needed to verify his identity by confirming his full card details and online banking password. They offered to stay on the line while Sam logged in to check if any unauthorised transactions had occurred.



Discussion questions:

What techniques is the scammer using to appear legitimate?

What should Sam do in this situation?

How can Sam verify if a call is genuinely from his bank?

Quick reference guide

Share these quick tips to help others implement cyber safety measures:

Password strength guide

- ✓ Use at least 14 characters
- ✓ Include uppercase and lowercase letters
- ✓ Add numbers and special characters
- ✓ Avoid personal information
- ✓ Use a different password for each account
- ✓ Consider a password manager

Phishing detection checklist:

- ✓ Check the sender's email address carefully
- ✓ Look for spelling and grammar errors
- ✓ Be wary of urgent requests or threats
- ✓ Hover over links before clicking
- ✓ Verify requests through official channels
- ✓ Never provide passwords via email

Safe device practices

- ✓ Keep software and operating systems updated
- ✓ Use anti-virus/anti-malware protection
- ✓ Enable automatic updates
- ✓ Back up important data regularly
- ✓ Lock devices when not in use
- ✓ Use encryption when available

Course conclusion

Congratulations on completing the Cyber Wardens Champions Course!

You now have the knowledge, tools, and resources to make a real difference in your community's cyber security awareness. Remember that cyber security is truly a team sport, and as a Cyber Wardens Champion, you're a key player in helping others protect themselves online.

Next steps:

1. **Choose your first audience:** Identify which group you'll start with – your workplace, professional network, or community group
2. **Select your approach:** Decide whether you'll begin with casual conversations or organise a more formal training session
3. **Gather your resources:** Review the scenarios, templates, and guides from this course that will best support your chosen audience
4. **Set a goal:** Commit to a specific, achievable goal (e.g., "I will help five colleagues set up multi-factor authentication this month")
5. **Connect with the Cyber Wardens community:** Join our online community to share experiences and stay updated on the latest threats and resources

Remember: Every conversation you have about cyber security helps build a safer digital world for everyone. Your efforts as a Cyber Wardens Champion truly matter.



Resources and references

Cyber Wardens official resources

A range of official tools is available to support your journey as a Cyber Wardens Champion. You can explore the main website for program information, access downloadable guides and communication materials in the resource library, and access the free online course catalogue to build your confidence and cyber knowledge.

- ✔ Cyber Wardens website: cyberwardens.com.au
- ✔ Resource library: cyberwardens.com.au/resources-content/guides-and-resources
- ✔ Cyber Wardens Courses: cyberwardens.com.au/courses

Additional resources

If you experience a scam or cyber attack, there are several trusted national services available to help. You can access step-by-step guides, report incidents, receive real-time alerts, and get expert phone support. Confidential assistance is also available if your personal or business information has been compromised.

- ✔ Small Business Cyber Security Guide: cyber.gov.au
- ✔ Report Cyber: cyber.gov.au/report
- ✔ Scamwatch: scamwatch.gov.au
- ✔ Stay Smart Online: staysmartonline.gov.au
- ✔ IDCARE: idcare.org
- ✔ Australian Signals Directorate Cyber Security Hotline: 1300CYBER1 (1300 292 371)

Thank you for becoming a Cyber Wardens Champion!

Remember, cyber security is a team sport,
and you're now equipped to be a key player in
protecting your community.