‘Tis the season for cyber safety

Your small business guide to cyber security for the festive season

Proudly supported by

Australian Government

COSBOA

CyberWardens.

Cyber safety to keep your business merry and bright

The holiday season is in full swing! Between Black Friday, festive promotions, and the New Year rush, small businesses are juggling extra orders, busy staff, and all the seasonal excitement. But this also makes it prime time for cyber criminals.

Scammers know the festive period is when small businesses are stretched the most. With so much going on, they hope you'll slip up, and the consequences can be costly: the average cost of a cyber attack to a small business is now $56,600, a 14% increase on last year's figures.

To help you get through the holiday period, we've prepared this guide packed with simple, practical steps to strengthen your digital defences, plus quick holiday-themed tips to keep your business and team safe online.

And don't forget: completing the free Cyber Wardens program is the perfect way to give the gift of cyber safety this festive season.

The top holiday cyber risks on Santa's naughty list

Cyber criminals never stop looking for ways to break into your business. Watch out for the top four cyber crimes impacting small businesses.

1.

Festive phishing emails

Scammers send emails posing as suppliers, delivery companies, or even holiday charities, hoping you'll click links or download attachments. These emails often use urgent holiday-themed language like "urgent order update" or "Christmas donation request."

2.

Fake online stores and deals

Too-good-to-be-true holiday deals can be a trap. Fake online stores pop up during the festive season, tricking businesses into paying for stock that doesn't exist, or stealing payment details. Always verify sellers and check reviews.

3.

Payment diversion scams

Scammers exploit the busy season by sending fake invoices or changing supplier payment details. With extra orders and holiday chaos, it's easy to miss, making it a perfect time for them to redirect your payments into their accounts.

4.

Vibe scamming

A newer scam on the rise, vibe scamming uses AI to mimic natural conversation and build false trust. Fraudsters craft highly convincing scams that "feel" genuine, making it easier to trick busy business owners and customers into sharing information or approving requests.

PRO TIP!

The Cyber Wardens Foundations module is a 10-minute introduction to the top cyber crimes, and the cyber security red flags that pose a threat to your business.

ENROL TODAY

cyberwardens.com.au/courses

12 cyber tips of *Christmas*

Spread some holiday cheer with the cyber version of a beloved Christmas carol, and help protect your business from cyber crime at the same time!

1. On the first day of Christmas...

...Keep your emails bright (and safe)

Cyber criminals will be sleighing through inboxes this season, using fake promotions and 'urgent' requests to get you to click on links. Keep email accounts secure, and make sure everyone on your team knows not to open unexpected links or attachments.

2. On the second day of Christmas...

...Set up multi-factor authentication (MFA)

Give your accounts the gift of added security. Adding MFA to your business apps and financial accounts can block unauthorised access. It's like putting a chimney cap on your digital house: only the right Santa can get in!

3. On the third day of Christmas...

...Wrap your Wi-Fi in security

When managing orders or payments away from the office, avoid using public Wi-Fi, as it can expose your information to cyber criminals. Instead, use a secure network or a virtual private network (VPN) for a layer of protection.

4. On the fourth day of Christmas...

...Don't open fake 'gift' invoices

Scammers often send fake invoices or fake refund requests, hoping you'll be too busy to notice. To sleigh this scam, always verify invoices directly with suppliers before paying.

5. On the fifth day of Christmas...

...Encrypt sensitive customer data

Customer data is a big target for cyber criminals. By encrypting and securely storing sensitive information, you're putting it under digital 'lock and key.'

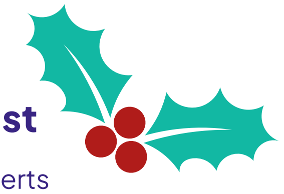
6. On the sixth day of Christmas...

...Lock down your social media

Fake customer complaints and 'order enquiries' can come through social media during the holidays. Be extra cautious when responding to messages from unknown contacts, and never click on suspicious links or open unexpected attachments.

7. On the seventh day of Christmas...

...Secure your banking info like Santa's naughty list



To prevent fraud, set up alerts for your business bank account, so you're instantly notified of any unexpected transactions.

8. On the eighth day of Christmas...

...Back up like a good little elf

Make data backups a routine practice, as cyber threats can strike when least expected. A recent backup will let you recover your data quickly if a scam or virus manages to get through.

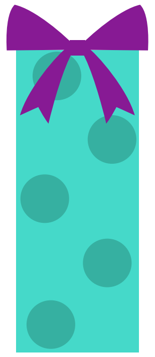
9. On the ninth day of Christmas...

...Give your accounts a festive shield!

Create long, strong and unique passphrases (like 'Presentsr3ind33rdancer@93!') instead of simple passwords (like 'Christmas2025'). Festive passphrases are harder for hackers to crack and add an extra layer of holiday security.

10. On the tenth day of Christmas...

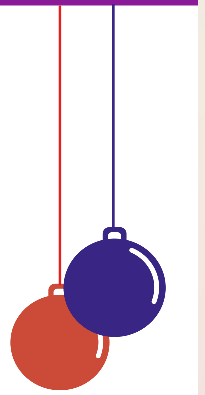
...Keep software up-to-date



Update patch vulnerabilities, keeping your business running smoothly and securely. Set your devices to auto-update so you're covered, even during busy periods.

11. On the eleventh day of Christmas...

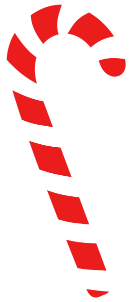
...Take a minute to stop, think, protect



When an invoice or email seems urgent, pause and reflect. Scammers rely on urgency. Take time to review details, ask a colleague, and stick to your normal payment process.

12. On the twelfth day of Christmas...

...Encourage the whole team to be cyber-wise



Cyber security is a team effort. Encourage your team to double-check anything that looks off and remind them to ask you if they're uncertain about a request.

How to *sleigh* a scam: Your AI holiday guide to cyber safety

This festive season, protect your business from AI-powered scams with reminders from Santa's holiday helpers to stay safe online.

Don't *'dash'* into AI-generated emails.

Be cautious of emails created by AI that look real but contain malicious links or attachments. Always verify the sender before clicking.

Dance carefully around AI chatbots and tools.

Not all AI tools are trustworthy. Only use verified platforms, and never share sensitive business or customer information with unknown bots.

Don't let AI impersonators *'prance'* around as your suppliers.

AI can create realistic fake invoices or messages. Confirm all requests through known contacts before making payments.

Verify before you trust AI tech support claiming to be *'vix-en'* your devices.

Fraudsters can use AI to impersonate IT providers. Only allow remote access when you initiated the call with a verified technician.

Don't *'comet'* to AI-generated requests

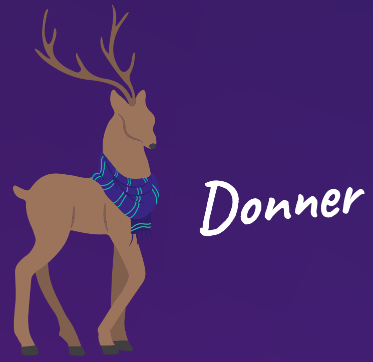
Urgent requests or AI-generated prompts may be scams. Stick to your normal business processes and double-check before acting.

AI may try to *'woo'* you into scams.

Be wary of overly persuasive AI-generated messages asking for sensitive information or unusual transactions.

'Don' your thinking cap before trusting AI recommendations.

Educate your team on AI-related scams and encourage them to question unusual requests, even if they look convincing.



Don't go *'blitzen'* through AI-generated invoices.

AI can produce realistic-looking fake invoices. Verify payment details carefully and double-check any changes with your usual contacts.

Follow your own *'red-nose'* instincts.

If an AI-generated message or email feels off, pause and verify independently before responding.

Give the gift of cyber security with Cyber Wardens

Cyber security doesn't stop with just one person —it's a team effort!

This holiday season, make sure your entire team has the knowledge and tools they need to keep your business safe online. Choose from our extensive course offering:

All courses are also offered in webinar format

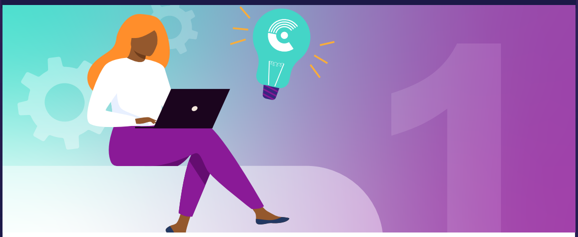
START HERE

Cyber Wardens **Foundations** 10 mins

Learn to spot cyber security red flags and essential strategies to protect your business.

Format:	Online course
Suitable for:	Busy business owners and employees

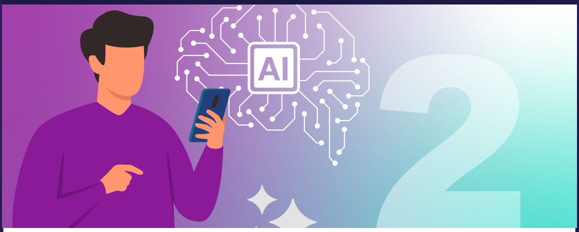
Cyber Wardens **Level One** 45 mins



Master four essential cyber security practices to protect your small business from common threats.

Format:	Online course
Suitable for:	Small businesses seeking improved cyber resilience

Cyber Wardens **Level Two** Safe AI for Small Business 30 mins



Simple and effective ways to keep small businesses safe from complex AI scams.

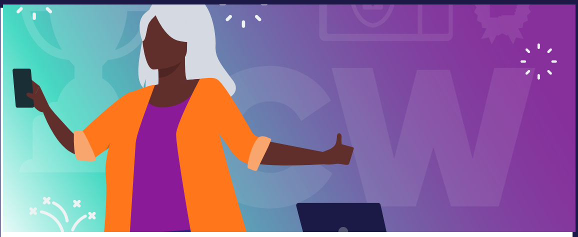
Format:	Online course
Suitable for:	Small businesses seeking a deeper understanding of AI's cyber security threats

Cyber Wardens **Level Three** Cyber Fit for the Supply Chain 30 mins

Strengthen your business's cyber security and meet the expectations of clients, partners and suppliers in your supply chain.

Format:	Online course
Suitable for:	Small businesses seeking to understand their critical role in the supply chain

Cyber Wardens **Champions** 45 mins



Help others stay cyber aware, build safer habits, and protect their business.

Format:	Online course
Suitable for:	Individuals seeking to help others become more cyber aware

Proudly supported by Australian Government COSBOA

CyberWardens.