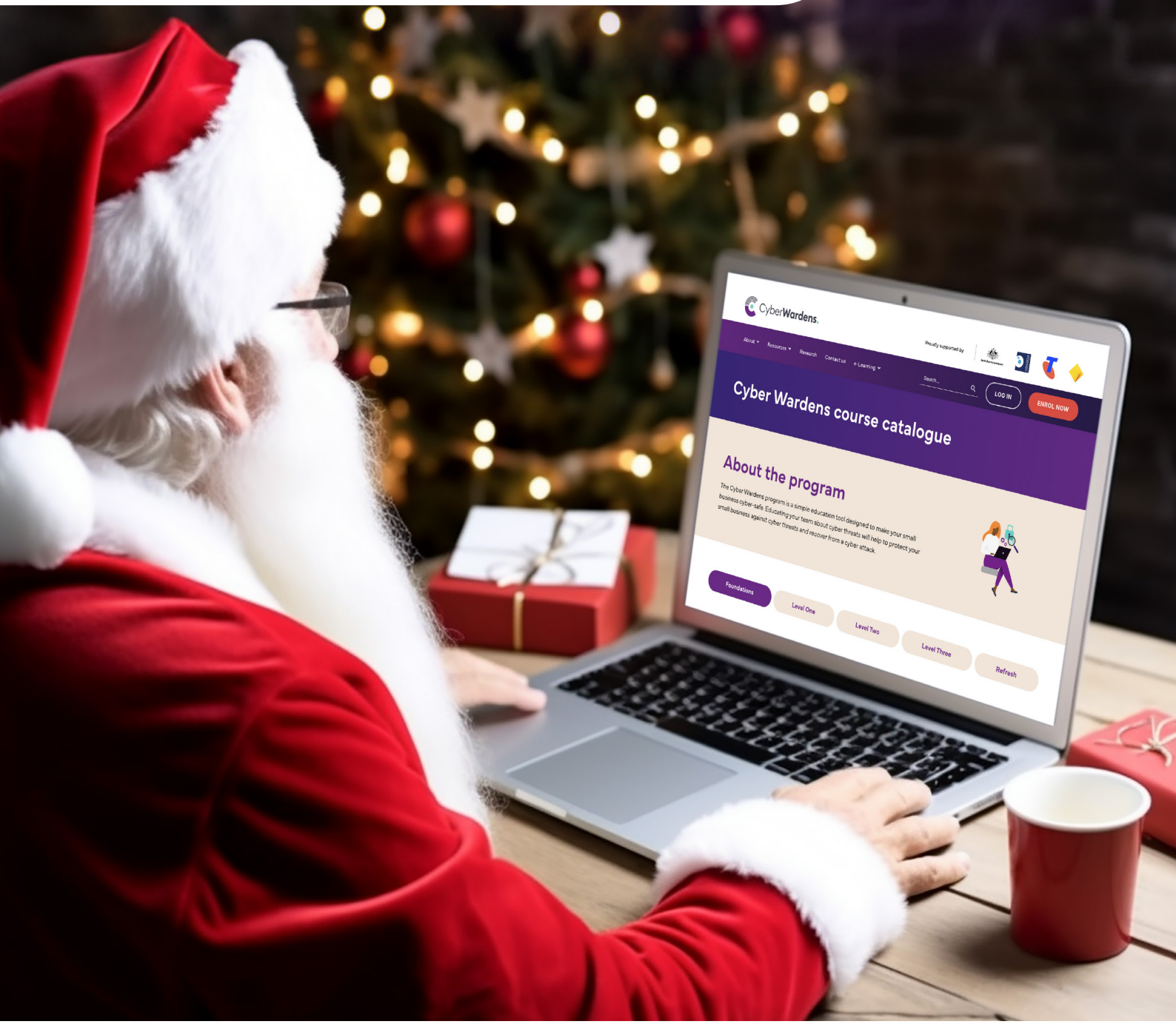
Deck the halls with **cyber safety!**

Your small business guide to cyber security for the festive season



Proudly supported by | Australian Government | COSBOA

CyberWardens.

The holiday rush is here!

Between Black Friday and the New Year, small businesses can face a mix of extra stock, bustling customer activity, and all the seasonal cheer — but these also make it peak festive season for cyber criminals.

Cyber criminals love this time of year. They know small businesses are juggling holiday orders, staff schedules, and last-minute to-dos, so they ramp up their efforts, hoping to catch you off guard.

With the average cyber attack costing $49,600 to a small business, and 43% of cyber crime targeting small businesses, now is the time to be vigilant!

This guide offers simple, actionable steps to help you bolster your digital defences, along with quick holiday-themed reminders to keep you and your team cyber-safe.

And to wrap it all up with a bow, don't forget to complete the Cyber Wardens program, a free online course designed to help protect Australian small businesses against cyber crime.

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 three cyber crimes impacting small businesses.

1.

Inbox break-ins

Business email compromise (BEC) attacks are just like a break-in in your inbox. Once inside, cyber criminals gain access to important information and can launch more damaging attacks.

2.

Fake invoices & payment redirection scams

Once they gain access to your inbox, scammers can trick your customers out of money by sending fake invoices that redirect payments to hackers.

They can also replicate supplier invoices with fake payment details that funnel money to their account rather than your genuine supplier.

3.

Banking burglary

Online banking fraud happens when cyber criminals access your bank accounts, allowing them to transfer out your hard-earned cash directly into their own account.

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!

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.

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!

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.

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.

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.'

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.

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.

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.

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 'Christmas2024').

Festive passphrases are harder for hackers to crack and add an extra layer of holiday security.

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.

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.

On the sixth 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

This festive season, sleigh the holidays with help from Santa's nine reindeer reminding you of the cyber security basics to stay safe online.

Avoid *dashing* through your emails!

Confirm the legitimacy of customer complaints and invoices and avoid opening links that look suspicious.

Dance right over to your IT team if something looks fishy.

Report anything suspicious to a trusted contact instead of handling it alone.

Don't let cyber criminals *prance* around pretending to be you.

Keep accounts secure with multi-factor authentication and automatic software updates.

If you need tech support or your devices need *'vix-en'*, only use trusted providers.

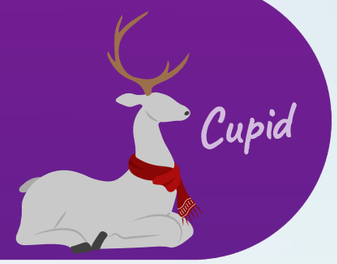
Never allow remote access to your computer unless you initiated the call.

Don't *'comet'* to any requests that seem out-of-the-ordinary

Be wary of urgent requests and stick to your regular payment processes.

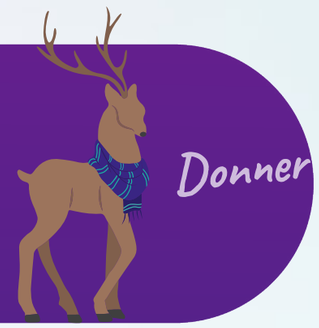
Customer *love* is great, but don't be too trusting.

Verify refund requests and ensure they're legitimate before you click on any links or open attachments.



Encourage your team to *don* their thinking cap before acting on a request online.

Educate them about holiday-season scams and empower them to question unusual requests.

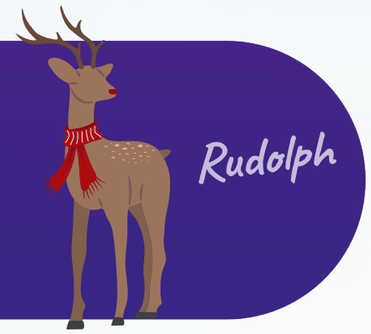


Blitzen through invoices can lead to errors.

Ensure every payment request is legitimate and accurately matches previous invoices, and always treat a change in supplier payment details with suspicion.

Don't be shy to be *"rude-olph"* when necessary.

If you're unsure of an email or call, double-check 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.

There are many ways for you and your team to complete the Cyber Wardens training. Choose from our expanding course offering:

CYBER WARDENS FOUNDATIONS

A 10-minute module helping you identify the cyber security red flags that pose a threat to your business

CYBER WARDENS LEVEL ONE

A short course introducing you to basic cyber security measures and actions to improve your cyber awareness

CYBER WARDENS FOUNDATIONS WEBINAR

An interactive session delivered weekly where participant can learn through live engagement with a Cyber Wardens educator

CYBER WARDENS REFRESH

Where Level One graduates can refresh their skills and knowledge while being introduced to new and emerging threats in the cyber landscape.

Visit cyberwardens.com.au/courses to enrol in *free* training and access resources to share with your team.

Join the Cyber Wardens community

This festive season, help protect your business by giving and receiving the **gift of free cyber security training!**

Proudly supported by Australian Government

CyberWardens.