CyberWardens.

Jingle all the way to cyber safety

The small business guide to simple cyber security through the festive season.

Proudly supported by

Australian Government

COSBOA

Cyber safety this Christmas season

For our small businesses, we know the lead-up to Christmas can be a busy and chaotic few weeks. It kicks off with Black Friday and doesn't let up until after Australia Day. We hope your business is enjoying a busy lead up to Christms and is ready for a successful summer ahead.

With extra stock coming in, an increase in customers and enquiries and more online orders, it's easy to get caught up in the day-to-day running of your business. If you do manage to squeeze in a holiday then you're trying to manage invoices or orders by yourself from places you might not usually work, like the beach!

Either way, the break in routine and increased tempo of the festive season make the Christmas and New Year period extra risky for managing your small business cyber security risks.

Cyber attacks on small businesses are rising at an alarming rate — a 23 per cent increase in the past 12 months. What's more, the average cost of cyber crime per incident rose by 14 per cent from 2021-22, to $46,000 for small businesses.

Aware of how busy the end of the calendar year can be for both business owners and their staff, cyber criminals are known to launch targeted attacks hoping you are too busy to spot the scam.

The Council of Small Business Organisations of Australia hopes this Cyber Wardens guide, which is focussed on cyber security at Christmas, helps you to stay cyber secure through one of the busiest trading periods of the year.

You'll find practical tips and quick wins that help you lock your digital doors this festive season and beyond.

If you haven't already, sign up your staff for the free Cyber Wardens training program. It's been designed by small businesses for small businesses so you can help protect your business against cyber threats and focus on what you do best.

Wishing you a Merry Christmas and a Happy New Year.

Luke Achterstraat,
CEO, COSBOA

Cyber Safety at Christmas

Common small business cyber attacks to watch out for this holiday season.

Cyber criminals never stop looking for ways to break into your business. The latest Australian Signals Directorate's (ASD) Annual Cyber Threat Report revealed the top three cybercrimes impacting small businesses.

Inbox break-ins

Email compromise attacks are like a break-in in your inbox. Once inside cyber criminals gain access to important information and can launch more damaging attacks.

Fake invoices and payment redirection scams

Business email compromise (BEC) fraud is a type of scam to trick you out of money or goods usually by sending fake invoices that redirect payments to hackers.

Banking burglary

Online banking fraud gives cyber criminals access to your bank accounts allowing them to transfer out your hard-earned cash.

What did the cyber security expert sing on Christmas Eve?

"I'm dreaming of a secure website!"

What to look out for this Holiday Season.

1 Scammers will try to take advantage of **how busy you are**

It's harder to spot a scam, fake invoice, or phishing attack when your to-do list is overflowing. Cyber criminals are relying on the Christmas hustle, hoping you will lose focus and miss things you might usually catch.

What to do: Slow down and be vigilant about following your standard cyber safety processes.

2 Scammers will try to send you **fake customer complaints**

Nobody likes disappointing customers. Fake customer complaints may be sent to your email or as private messages on social media and include accusations of damaged or missing goods with a link to download a 'photo'.

What to do: Be alert to unusual file types as the link may contain computer viruses or phishing attacks.

3 Scammers will try to **send you fake invoices**

While businesses are busy, scammers take the chance to ramp up fakes. Fake invoices, fake stock or supplies, fake refund requests, fake links, fake tech support, fake charities. They hope you will process the request during the busy period. According to Xero, nearly one in five Australian small businesses has been a victim of invoice fraud, falsely paying out huge sums ($15,500 on average).

What to do: Check invoices with two people.

4 Scammers will try to **target your staff as well**

Cyber security is a whole-of-team sport — everyone can be a target, and everyone has a role to play in spotting and stopping attacks. You should regularly remind your staff that if they're unsure if an invoice, email or call is from a legitimate source, they should raise it with you. Empower them to say no and escalate.

What to do: Talk to your team about the heightened risk of cyber attacks at Christmas. Remind them it's good to double-check anything suspicious.

How to sleigh a scam...
with Santa's nine reindeer

Try not to let customer complaints **dash-er** your hopes, they may not be legitimate!

- Confirm you are dealing with a legitimate customer.
- Don't click on supposed links to photos that might hide malicious software.
- Be alert to urgent requests pressuring you to transfer funds.

Don't let someone **dance-r** through your computer.

- Do not give anyone access to your computer or information unless you trust them and know them.
- Upgrade from passwords to longer passphrases.
- Set a unique passphrase for every account (no double-ups and no shared passwords).
- Use a password manager to safely store passwords.

Protect yourself so a scammer can't **prance-r** around pretending to be you.

- Protect your online accounts by using multi-factor authentication whenever it is available.
- Set your apps, plug-ins and browsers to auto-update so you are working with the latest software security updates.
- Shut down and restart regularly so your auto-updates are installed.

Don't always be a **cupid** for your customers.

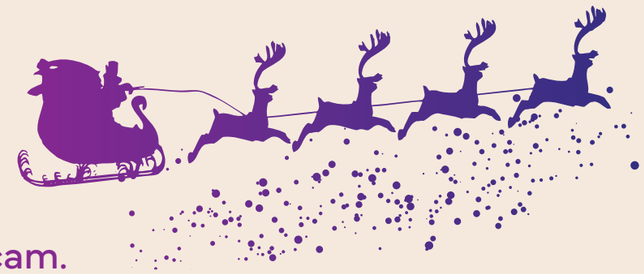
We know every small business loves its customers and is grateful for their support. That's why you might fall victim to a refund request scam.

- Ensure the refund request is for a legitimate item or service.
- Refund scams occur when buyers purchase items and then ask for a refund or allege they have mistakenly overpaid you.
- Check every refund request to ensure the money is going back to the same card used for the original purchase.
- In cases where the initial transaction was made with a fraudulent card, you'll likely be obliged to return the funds from the original transaction.
- You will also be out of pocket for the money you refunded to the scammer.

Avoid **blitzen** through your invoices.

Christmas is a busy time, we know that. But, sometimes, it pays to sit down and go through your outstanding invoices slowly.

- Double-check every invoice.
- Ensure the business is legitimate.
- Ensure the invoice matches previous invoices.



Avoid **comet-ting** into a scam.

- Be wary of urgency. Exercise caution whenever someone insists that you must act immediately, as scammers often attempt to create a sense of urgency to manipulate you into complying with their requests.
- Stick to your usual payment handling process.
- Slow down and review every supply or stock order coming through your business — you never know when one of these might be a false or low-quality stock offering from a scammer trying to make a buck.
- Watch for red flags such as a strangely configured email address, unusual requests, unexpected invoices, "confidential" requests or unsophisticated language and typos.

If you're having tech issues, only trust a regular supplier you can verify to **vix-en** your computer.

- If you're contacted and offered technical support or if you put out a call out for technical help, be aware that not everyone who offers you assistance will be genuine.
- Never give out sensitive details to unverified providers.
- Never allow remote access to your devices if you have been contacted unexpectedly.
- If you are not able to vix-en your devices, be careful when disposing of them!

Remind your staff to **don-ner** their thinking caps because a scammer might target them too.

- Confirm invoice details directly with suppliers using a trusted contact number.
- If staff are being pressured to pay an invoice they don't recognise or have assumed is for the business owner or another colleague, tell them it's okay to think twice and come to you if they're unsure.
- Don't trust calls, letters, emails, or messages on social media from someone who says they can recover money you lost in a scam for a fee.

Don't be afraid to be **rude-olph**.

It's okay to hang up the phone or not reply to an email or text message if you're not sure who is contacting you.

- Don't call them back on the number they gave you.
- Check the business or organisation's contact details independently.
- Do this by looking up their website and contact details online.
- Be a Secret Santa and report the attempt to https://www.cyber.gov.au/report-and-recover/report

Cyber attacks are more common than you think

Don’t leave your business unprepared this Christmas.

Cyber Wardens training, for you and your team, will help protect your business and help lock your digital doors. In fewer than 45 minutes the free Cyber Wardens program will give your small business quick wins in cyber security.

Learn how to:

Defend against digital break-ins with **up-to-date software**

Set a virtual alarm system with **MFA (multi-factor authentication)**

Password like a pro by upgrading to **passphrases**

Bounce back with **backups**

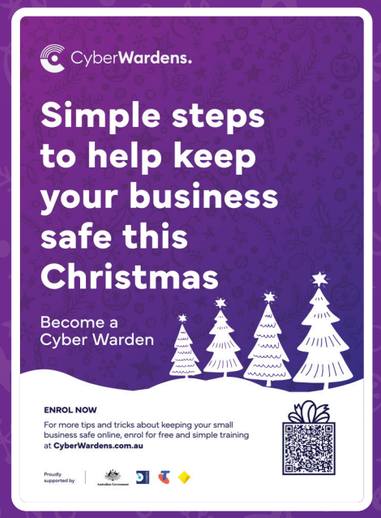
Enrol today.
www.cyberwardens.com.au

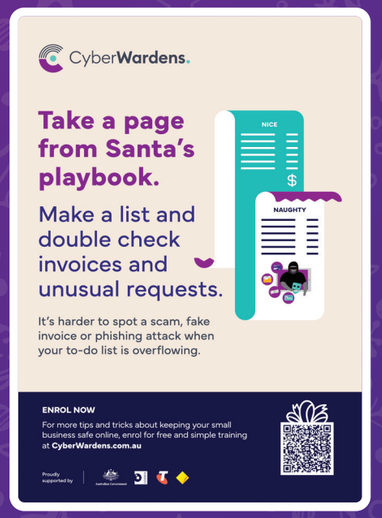
Cyber safety is a team sport

As a Cyber Warden, it’s your job to make sure everyone on your business team has the simple skills needed to spot a scam and catch it before they click.

To help your team stay cyber safe this holiday season, Cyber Wardens have a kit of posters and resources to share with your team.

DOWNLOAD YOUR HOLIDAY SAFETY KIT





You can find more helpful resources by visiting

cyberwardens.com.au/resources

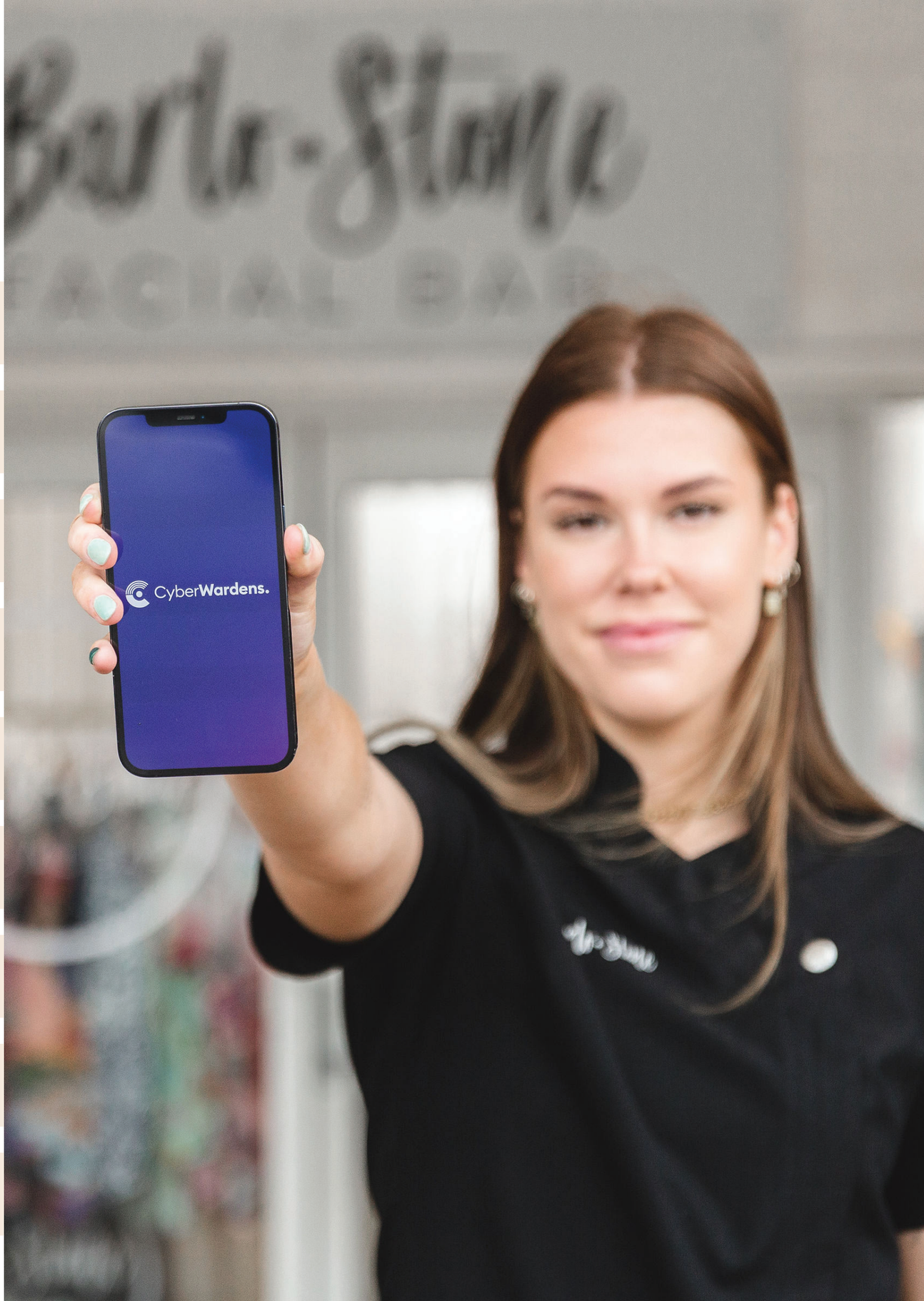
Why did the elf refuse to click on any suspicious email links?

He didn’t want to get wrapped up in a phishing scam!

CyberWardens.

Christmas to-do list

- [ ] **Complete** the free Cyber Wardens training
- [ ] **Print** a Cyber Wardens Christmas Safety poster for the office
- [ ] **Email** your team with a reminder about how to stay cyber safe at Christmas
- [ ] Have team members **subscribe** to the Cyber Wardens email
- [ ] **Follow** on social media for simple small business safety advice
- [ ] **Look** twice at unexpected invoices (ask a colleague or trusted friend if you're not sure)
- [ ] Take a deep breath and **high-five** yourself for getting through another festive season
- [ ] _____
- [ ] _____



CyberWardens.

Proudly supported by

Australian Government

COSBOA

Equip your business with Cyber Wardens training.

It's a simple and free educational tool designed to build a cyber-smart small business workforce.

Cyber Wardens is an initiative of the Council of Small Business Organisations of Australia, supported by the Australian Government and an industry alliance led by Telstra, CommBank and the Australian Cyber Security Centre.

Learn more at cyberwardens.com.au