CyberWardens.

Tax time is prime time for cyber crime

Be prepared for EOFY with this cyber security guide for small businesses

COSBOA COUNCIL OF SMALL BUSINESS ORGANISATIONS AUSTRALIA

cyberwardens.com.au

Cyber criminals are getting busy this EOFY. Know how to stop them in their tracks.

Cyber criminals know this is an intense period for small businesses. Make sure you and your team are prepared.

The end of the financial year (EOFY) and tax time mean more work, reporting, and financial activity. As well as managing your usual tasks, you may be dealing with EOFY sales, payroll changes, asset write-offs, superannuation updates, and tax returns. It's a lot, and cyber criminals know it.

Scammers take advantage of this busy period

Research from CommBank indicates that one in four Australians have encountered or experienced an EOFY-related scam. These scams predominantly involve impersonations of the Australian Taxation Office (ATO), myGov, and various financial institutions, using emails and SMS messages to deceive recipients.

Many small businesses think they're too small to be targets

Cyber criminals are focusing more on small businesses. The average cost of a cyber attack on a small business is $49,600[1]. Recent research from Cyber Wardens reveals that four in five (82%) small businesses have either experienced or been exposed to a cyber incident[2]. Concern is also growing, with 82% of small business owners and employees now worried about the impact of a cyber attack, scam or hack on their work or business, up from 77%[2].

To help you stay safe this tax time, Cyber Wardens has created this quick EOFY Cyber Security Guide.

It covers:

- How to spot ATO and myGov scams
- AI-powered EOFY threats
- Ways to protect against common scams
- A checklist to keep your business cyber-safe

We encourage you and your team to complete the Cyber Wardens training before EOFY.

Cyber security is a team effort.

Be part of the Cyber Wardens community and protect your business today.

Luke Achterstraat
COSBOA Chief Executive Officer

[1] ASD Cyber Threat Report 2023–2024
[2] Cyber Wardens Small Business Cyber Security Pulse Check Report

How cyber criminals can attack

The average cost of a cyber attack to a small business is $49,600

INCREASED SCAM ACTIVITIES AT EOFY & TAX TIME

Fake ATO
Impersonation emails, SMS and call scams to steal money

Fake myGov
Fake links or calls to steal access to your myGov account

Transfer scams
Fraud links and invoices that trick you when you're busy

Data breach
System hack to access data between you & accountant/ bookkeeper

MAJOR THREATS INCREASE IN FREQUENCY AROUND EOFY

Inbox break-in
Criminals gain access to important information and launch damaging attacks

Payment redirection
Business email compromise tricks you out of money or goods usually via fake invoices or emails

Cloud compromise
Criminals hack into your storage to access and control business data

Banking burglary
Online banking fraud gives access to your accounts and your savings

Watch out for ATO and myGov scams

Stay vigilant: ATO and myGov scam alerts

As tax time approaches, it's important to be cautious of unsolicited emails, phone calls, text messages, or social media communications claiming to be from the ATO or myGov. If you're not sure about the authenticity of a message, do not engage with it.

> **In April 2025 alone, the ATO received 6,189 reports of impersonation scams. Notably, 96.5% of these scams were conducted via email, and 2.8% via SMS[3].**

Remember, the ATO will never send unsolicited messages containing hyperlinks or request personal information via email or SMS. Always access ATO services directly by typing ato.gov.au or my.gov.au into your browser.

Staying informed and vigilant is your best defense against tax-related scams

myGov and ATO online account fraud

In early 2025, the ATO reported a rise in identity fraud cases involving phishing scams, data breaches and insecure home networks. In the case of Perth resident Kate Quinn, scammers used stolen personal information to lodge a fake $8,000 tax return. By changing the bank details linked to the victim's account, they were able to divert the refund before the fraud was detected.

myGov impersonation scams

Scammers are taking advantage of the change of service name from **myGovID** to **myID** to trick the community into thinking they need to reconfirm their details via a link.

The link directs users to a fraudulent myGov sign-in page where scammers steal sign-in credentials and use them for identity theft or other fraudulent activity such as refund fraud.

Stay safe this end of financial year

Be wary of emails, phone calls and text messages claiming to be from the ATO. If you suspect you've received a scam message or have inadvertently provided personal information to a scammer, it's essential to act straight away:

Report the incident

Forward the suspicious email to **ReportScams@ato.gov.au** or take a screenshot of the SMS and email it to the same address.

Contact the ATO:

If you've shared sensitive information or made payments to a scammer, call the ATO's dedicated scam line at **1800 008 540.**

[3] Australian Taxation Office

AI-powered scams:

The new EOFY threat for small businesses

EOFY is a busy time, and scammers know it. Cyber criminals are now using artificial intelligence (AI) to create more convincing and targeted scams, especially when small business owners are under pressure.

Fake emails and invoices

AI can generate emails or tax invoices that look like they're from the ATO, your accountant, or suppliers.

Impersonation scams

AI can mimic real voices or writing styles to impersonate someone you trust, like a team member or service provider.

Personalised phishing attacks

Scammers use AI to pull public info (like your business name, ABN or social media posts) to tailor their attacks and make them more believable.

Urgent requests around payments or logins

Many AI-generated scams use tax-time language to trick you into clicking a link, paying a fake bill, or handing over sensitive details.

Cyber security is a team sport

> Cyber security is a team effort right across the small business ecosystem. Your bookkeeper and accountant are key members of the team, working with small business owners and their suppliers.

Bookkeepers and accountants are vigilant when it comes to protecting data and financial information. They have seen the hardship that cyber attacks can cause small businesses - the financial losses, personal stress and reputational damage.

> That is why the Institute of Certified Bookkeepers Australia recommends the Cyber Wardens cyber security training for all small businesses."

— Matthew Addison | ICB Executive Director and COSBOA Chair

DID YOU KNOW?

Only **41**% of small businesses feel confident their business is protected from emerging threats, such as AI-driven attacks.

95% cyber attacks involve human error. **Make sure everyone on your team knows how to recognise cyber red flags by completing the Cyber Wardens training.**

6 ways scammers target you and how to stop them in their tracks

Technology is vital to your small business and managing your finances, especially during the EOFY rush and tax time. Here are 6 things to look out for and what to do to stay safe online.

Cyber criminals will take advantage of how busy you are

What to do:

- Don't act on urgent emails immediately
- Stick to usual banking and payment processes
- Watch for unusual email addresses, unexpected invoices, and typos
- Be alert to urgent transfer requests

Hackers will get a pay day from your poor processes and weak passwords

What to do:

- Use multi-factor authentication on important accounts
- Set auto-updates for apps, plug-ins and browsers
- Restart regularly to install updates
- Use unique passphrases for each account
- Use a password manager

Scammers will send you fake invoices or demands

What to do:

- Double-check all invoices against previous ones
- Verify business legitimacy before paying
- Don't click suspicious links or unusual file types

Scammers will pretend to be a customer or supplier requesting a refund

What to do:

- Verify refund requests are legitimate
- Ensure refunds go back to original payment method
- Report any cyber attacks immediately

Scammers will try to access your computer and data

What to do:

- Only trust verified tech support providers
- Never give remote access to unverified callers
- Factory reset old devices before disposal

Scammers can target your staff and family to break into your business

What to do:

- Educate family and staff about EOFY scam risks
- Always verify invoice details with trusted supplier contacts
- Encourage staff to check with you before paying unfamiliar invoices

Your handy EOFY cyber security checklist

- [ ] Create long, strong and unique passwords or upgrade passwords to passphrases
- [ ] Enable multi-factor authentication on all your accounts
- [ ] Install automatic software updates on all your devices
- [ ] Back up your data with cloud-based and portable storage drives
- [ ] Regularly discuss cyber security with your team and suppliers
- [ ] Always look twice at invoices and emails and verify with the sender if you're unsure
- [ ] **Complete the free Cyber Wardens training:** cyberwardens.com.au/courses
- [ ] Encourage everyone in your network to complete the Cyber Wardens training - one weak link in your supply chain could cost you nearly $50,000
- [ ] **Know how to report a cyber crime:** go to cyber.gov.au/report-and-recover/report or call the Australian Cyber Security Hotline on 1300 CYBER 1

DID YOU KNOW?

82% of Australian small businesses experienced a cyber incident in 2024.

A cyber crime is reported every **6 min** in Australia

The Cyber Wardens program is designed to be accessible to all Australian small businesses.

With options for self-paced e-learning, and live and on-demand webinars, you can train in a learning style that suits you.

ENROL NOW

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 Aid for Health Professionals — 30 mins

Specialised training to help medical professionals protect sensitive patient data from cyber threats.

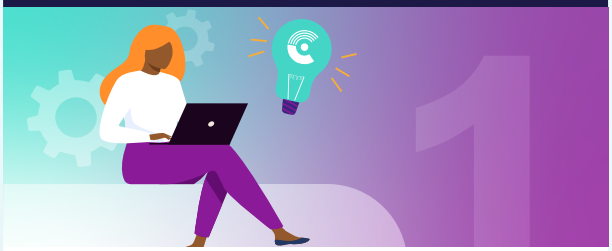
Format:	Live or on-demand webinar
Suitable for:	Healthcare professionals and support staff

Cyber Wardens **Foundations Webinar** — 30 mins

Expert-led session covering key cyber risks, warning signs, and practical security steps for small businesses.

Format:	Live or on-demand webinar
Suitable for:	Business owners and employees who prefer interactive, guided learning

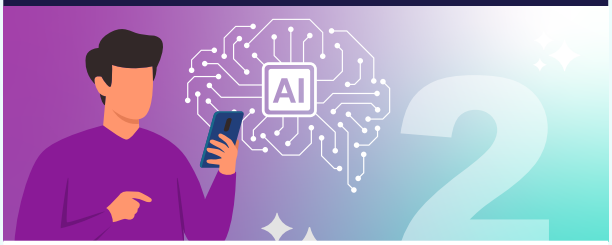
Cyber Wardens **Level One** — 30 mins



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

CyberWardens.

Proudly supported by | Australian Government | COSBOA