CyberWardens.

15 April 2025

Media Release

Hunt out the bad eggs scamming small businesses this Easter

Cyber Wardens launches holiday campaign as new research reveals rising fears over AI-fuelled attacks

Research highlights

1. A new Cyber Wardens report reveals **nearly half** (41 per cent) of operators lack confidence in fending off AI-driven incidents.
2. More than **7 in 10** (74 per cent) think rapidly advancing technology, including AI, pose a risk to their small business in the next five years.
3. **4 in 5** small businesses experienced a cyber incident in the past 12 months.
4. Cyber security is seen as a bigger threat to small businesses than energy prices.

15 APRIL 2025: Small businesses are being warned to watch out for bad eggs during the Easter period in a new campaign highlighting hidden cyber threats.

Cybercriminals are out in force during the holiday seasons, and COSBOA's Cyber Wardens program is raising awareness of increased risks often disguised in 'shiny packaging'.

The campaign comes as new research launched today reveals small businesses now view cyber security as a more significant threat to small businesses than energy prices.

The Cyber Wardens study has revealed a rising level of concern among small businesses about cyber crime, as figures show a spike in incidents in the past year.

The study found 4 in 5 (82 per cent) experienced a cyber incident in the past 12 months, while the number of small business owners and employees concerned about online crime jumped 5 per cent to 82 per cent.

Only 2 in 5 (41 per cent) felt confident their business was protected from emerging threats such as AI-driven attacks and ransomware.

Cyber Wardens is a national initiative of the Council of Small Business Organisations of Australia (COSBOA), supported by the Australian Government and an industry alliance, to help protect Australia's small businesses from online threats.

To help protect small businesses from the rising threat of AI scams, Cyber Wardens is launching a new course offering, Safe AI for Small Business, later this month.

COSBOA CEO Luke Achterstraat said Australian small businesses needed to be on heightened alert during Easter, particularly given the challenges posed by emerging technologies such as AI.

"Cybercriminals know that small businesses and their staff can be extra busy in the lead-up to holiday periods such as Easter, and may let their guards down. And just like Easter eggs, cyber threats in the AI era can come wrapped in shiny, appealing packaging to try to trick you," he said.

"Our new Cyber Wardens research shows that incidents are increasing, and emerging technologies such as AI are compounding concerns for already-stretched Australian small businesses.

"Cyber attacks on small businesses can cause devastating financial loss and personal distress for owners, employees and customers. That's why the Cyber Wardens program for owners and employees is such an important initiative."

On a positive note, he said there were some encouraging results from the research, which has been conducted once a year since the program kicked off in 2023.

"Since our first year of research, there has been a 12 per cent drop in small businesses categorised as being the least aware and active on cyber security. There has also been fantastic progress in using strong passwords and passphrases."

More than 1,500 small business owners and employees participated in the 2025 Small Business Cyber Security Pulse Check Report, to measure and map small business cyber security behaviours and attitudes.

More than 1 in 2 (54 per cent) see cyber security as a medium or high risk to their business in the next five years, up 5 per cent from Year 1 (49 per cent). It ranked as the third highest

threat behind economic instability (67 per cent) and cost of staff (56 per cent), with energy prices less of a concern in fourth (52 per cent).

Rebecca Warren, Executive General Manager for Small Business Banking at CommBank, a founding partner of Cyber Wardens, said it was important to keep up with the trends as scams constantly evolved and became more sophisticated, particularly with the growing uptake of AI.

“For example, traditionally, phishing involved scammers sending dodgy-looking emails or texts with suspicious links in an attempt to trick you into sharing personal details, including bank or email account information and one-time security codes,” she said.

“We’re now seeing AI-powered scams that mimic human interaction with alarming accuracy. From lifelike impersonations to near-perfect email imitations, scammers are adapting to trick time-poor business owners into sharing confidential information or approving fraudulent transactions.”

With scammers now leveraging AI to create highly sophisticated and convincing communications, making it even harder to identify fraudulent activity, Ms Warren said it was more critical than ever to upskill on cyber safety and scam awareness.

Mr Achterstraat said the findings clearly showed the Cyber Wardens program was having a positive impact and helping ensure small businesses understood the importance of securing business and personal data.

The Cyber Wardens program offers a range of course options, including a 10–minute Foundations course, webinars and a Cyber Aid offering, which has been tailored to small healthcare businesses.

For information on the range of courses available, visit cyberwardens.com.au.

The Small Business Cyber Security Pulse Check report can be downloaded here.

Media enquiries: media@cyberwardens.com.au, or 0466 027 957.