Media Release

19 January 2024

Risky Business: New research reveals top five everyday habits making small businesses a target for cyber crime.

Out with the old and in with the secure. New research reveals the top 5 everyday habits that make small businesses more vulnerable to cyber-attacks and easy steps to avoid them in 2024.

January 19, 2024: The cyber security of a small business is only as strong as the good habits each team member practises, yet nearly four in five small business owners (78%) have observed everyday habits occurring that inadvertently make them more vulnerable to cyber crime.

As workers get back to work for 2024, it's crucial small business teams stay vigilant and adopt cyber-safe habits this year.

New research from the Council of Small Business Organisations of Australia's (COSBOA) Cyber Wardens program has revealed the top 5 cyber security bad habits prevalent among Australian small businesses.

The study, based on a survey of more than 2,000 Australian small businesses, highlights common pitfalls that could expose them to potential threats, data breaches and financial losses as they return to work from the summer holidays. The findings aim to raise awareness and empower small business owners to enhance their cyber resilience by building simple cyber-safe habits into their daily business lives.

"It's hard to remain vigilant, so this is a reminder on how to avoid slipping into bad habits and instead build good habits that improve your business culture of simple cyber security," COSBOA CEO Luke Achterstraat said.

"Through the Cyber Wardens program, we are encouraging small business owners to make simple swaps in the everyday habits of their businesses as the easiest way to kickstart your new year cyber safety plan."

Kirsten Lynch, Owner of Plato's. Wonder. Create. Discover — a gift and toy shop in central Hobart — said she and her staff had been guilty of sharing passwords among themselves and across different programs, but, after completing the Cyber Wardens training, they had made changes to ensure everyone had their own strong, unique passwords.

“Running a small business, I know just one attack could mean the end of my business, so I take cyber security very seriously,” Ms Lynch said.

“I think the Cyber Wardens program is an informative, simple tool all businesses can use to help prevent cyber crime affecting their businesses. I’ll be asking all my staff to do the training.”

5 good habits to help keep your small business safe from cyber-attacks

Shut down your computer instead of putting it in ‘sleep mode’ 1 in 4 (27%) small businesses put their computers in ‘sleep mode’ rather than shutting them down, increasing the risk of out-of-date software giving access to cyber criminals.	***Cyber-safe habit #1:*** When we shut down our computers, automatic software updates are installed that can help protect against a cyber break-in. Try to shut down your computer every night when you finish work.
Use long, strong and original passphrases Passwords are your first line of defence, yet 1 in 4 (26%) reuse the same passwords across multiple systems and platforms. About 16% of small businesses also use short passwords, making them easier to crack.	***Cyber-safe habit #2:*** When we use unique and complex passwords or passphrases, we stop cyber criminals from accessing multiple programs and services if they crack one of them. Change your passwords, including for your company email, financial services, business files and any accounts storing your payment details and save them in a secure password manager.
Identify and report suspicious emails More than 1 in 5 (21%) small businesses are deleting suspicious emails they think could be scams without alerting IT or the head of their business.	***Cyber-safe habit #3:*** Sharing suspected scams with the right people helps to ensure the senders can be investigated and blocked, and that other staff can be warned about these attempts. You can also report scams to the National Anti-Scam Centre — Scamwatch — or the company being impersonated, such as your bank or phone company.
Give team members unique logins 1 in 5 (20%) small businesses share passwords between team members.	***Cyber-safe habit #4:*** When each team member has their own unique login, it means that if one staff member’s password is compromised, multiple accounts aren’t compromised. You are also better protected from insider threats.
Action updates ASAP 1 in 5 (18%) of small businesses are ‘snoozing’ software updates.	***Cyber-safe habit #5:*** It is hard to action software updates when you’re busy— they always seem to pop up when you’re the most stressed! But making updates a priority means you will deliver important bug and security fixes as soon as they become available. Hackers use these security weaknesses to attack your systems, so the sooner you action updates, the sooner you’ll be protected.

Cyber Wardens urges small businesses to make simple swaps in the everyday habits of their businesses to kickstart their new year cyber safety plans and foster a culture of awareness.

The free, Australian Government-funded Cyber Wardens program provides training to small business owners and employees on how to digitally safeguard their businesses. This includes essential upskilling on the fundamentals of multi-factor authentication, password management, device updates and backups.

According to Scamwatch, Australians lost more than $429 million to scams in 2023, with phishing, false billing, online shopping scams and identity theft the most commonly reported scams.

Last year the ACCC reported the number of businesses losing money to scams had increased by 73%.

The latest Australian Signals Directorate's (ASD) Annual Cyber Threat Report revealed the average cost of cyber crime per incident rose by 14 per cent from 2021–22, to $46,000 for small businesses.

Start the new year with good habits to help protect your small business!

For more information, please visit www.cyberwardens.com.au

Additional Quotes

Amanda Hutton, Group Executive of Telstra Business

"For a business owner who's already juggling a lot of different responsibilities, getting on top of cyber security can feel overwhelming, and while Telstra's Cleaner Pipes initiative is working to help stop scams before they hit our customers, we know some can still slip through. That's why COSBOA's cyber-safe habits are so helpful because they break the task of improving cyber security down into simple improvements that have a big impact.

"Telstra encourages all small businesses who want to improve their cyber resilience this year to enrol in the free Cyber Wardens program, which is full of excellent resources and simple tips to help you and your team build strong cyber-safe habits."

Rebecca Warren, Executive General Manager Small Business Banking, Commonwealth Bank

"Scams and fraud can have a devastating impact on small businesses, both financially and emotionally.

"While the prevalence of scams continues to rise, recent CommBank data shows anti-scam initiatives announced by the bank over the past year are making a real difference for customers, with CommBank protecting retail and business customers from more than $228 million scam attempts through its early prevention and detection program.

"People are the first line of defence when it comes to payment scams which is why the Cyber Wardens program to upskill small businesses in cyber safety, so small businesses can build resilience from the ground up, is such an important initiative."

ENDS

Background

About Cyber Wardens

At Cyber Wardens, we are on a mission to ensure Australian small businesses operate in a cyber-safe environment.

By bolstering the cyber capabilities of people who work in small businesses, we make it easier for small businesses to increase their cyber posture to prevent attacks and be resilient to them. Our goal is simple — for cyber criminals to consider Australia 'closed for business'.

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 led by Telstra, CommBank and the Australian Cyber Security Centre, to help protect Australia's 2.5 million small businesses from online threats.

Cyber Wardens are the digital equivalent of first aid officers or fire safety wardens. They are equipped to prevent, prepare, fight and help recover from a cyber attack such as the theft of customer data or intellectual property.

Just as we physically protect ourselves by locking up our businesses and homes at night, the Cyber Wardens program will give small businesses the skills to shut their digital doors to lurking cyber threats.

Leveraging COSBOA's grassroots infrastructure and reputation to change the behaviours of Australia's 2.5 million small businesses, the free Cyber Wardens program uplifts small businesses by educating an in-house cyber safety officer to build cultural competencies alongside technical know-how.

By bolstering the cyber capabilities of people who work in small businesses, we make it easier for small businesses to prevent and recover from cyber-attacks.

Cyber Wardens will complement Australia's growing pool of cyber technical experts to drive cultural change and cyber-safe mindsets in Australia's small businesses.

The Cyber Wardens program works in conjunction with two new initiatives recently announced by the Albanese Government: $7.2 million to establish a voluntary cyber health-check program that will allow businesses to undertake a free, tailored self-assessment of their cyber security maturity, and $11 million in the Small Business Cyber Resilience Service which will provide one-on-one assistance to help small businesses navigate their cyber challenges, including walking them through the steps to recover from a cyber attack.