CyberWardens.

Risky Business

The everyday habits increasing small business cyber risk

A Cyber Wardens Research Report

JAN 2024

Proudly supported by

Australian Government

COSBOA

Making cyber security a habit

You can simplify your small business cyber security by building good everyday habits to increase cyber safety and decrease the chances a cyber criminal can break into your business.

Making simple swaps in the everyday habits of your business is a powerful strategy to build a culture of cyber safety, ultimately reducing the likelihood you will suffer a devastating digital break-in.

Bad habits observed in most small businesses

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

Almost 20% of small businesses keep their **passwords written down** somewhere.

Almost 1/4 of small businesses **share passwords** with colleagues.

Everyday habits can create a risky business system

Once bad habits creep in, they tend to continue unless you take measures to stamp them out. They are likely to become embedded in the ways a business works, increasing its risk of a cyber incident.

Each habit is significantly more likely to occur ‘sometimes’ or ‘almost always’, than ‘rarely’ or ‘never’.

Once observed, everyday habits are persistent

	Never or **Rarely** observed	**Sometimes** or **Almost Always** observed
Keeping a password document	16%	**83%**
Putting a laptop in ‘sleep mode’ over shutting down	16%	**83%**
Re-using passwords	17%	**82%**
Sharing a single login between casual staff	19%	**79%**
Sharing passwords between colleagues	21%	**78%**
Paying for one software licence and sharing logins between people	22%	**77%**
Snoozing a software update	26%	**73%**
Using short passwords	26%	**73%**
Downloading personal software onto a work phone or computer without IT approval	28%	**71%**
Allowing a family member (non-employee) to use a work phone or computer	29%	**71%**
Suspecting an email on a work computer was a scam and deleting it without alerting IT	31%	**69%**
Creating business documents that aren’t backed up	32%	**68%**
Adding personal details such as travel plans to an ‘out-of-office’ response	36%	**64%**

Risk spotters on high alert

Anyone can be a Cyber Warden and help prevent cyber attacks. Just like work health and safety (WHS) officers help keep small businesses safe from physical hazards, Cyber Wardens use the same skills to prevent and protect against digital threats. A trained Cyber Warden knows the unique cyber hazards and risks of your business.

Four audience segments were most likely to be alert in observing bad habits sneaking into your small business team.

Millenials

Women

Larger small business teams (5-19 employees)

Owners and CEOs

Employees spot password vulnerabilities more than bosses do

Team members were more likely to see and spot basic password vulnerabilities.

24% of small business employees have **observed colleagues sharing passwords** compared to only **15% of owners and CEOs**

16% of employees report a **shared casual login** compared to just **12% of small business owners and CEOs**

Cyber safety starts with small business owners

THREAT: Hackers use one password to enter all your business systems and accounts	**THREAT:** Family members may accidentally compromise your device to cyber criminals	**THREAT:** Unable to recover important business data in the event of an attack
Reusing passwords	**Sharing devices with family members**	**Creating business documents that aren't backed up**
30% of owners admit to reusing passwords compared to just 22% of team members	Owners are almost twice as likely to share work devices with family members compared to employees	Business owners are more likely (17%) to observe important business documents not being backed up, compared to 13% of employees

New research reveals top 5 cyber bad habits among Australian small businesses

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.

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

Shut down your computer instead of putting it in ‘sleep mode’

More than 1 in 4 (27%) 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:

Shut down computers

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. And **16%** of small businesses use short passwords, making them easier to crack.

Cyber-safe habit #2:

Upgrade passwords to passphrases and protect them in a password manager

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.

5 good habits to help keep your small business safe from cyber attacks (cont...)

Report suspected scams

More than 1 in 5 (21%) delete suspicious emails they think could be scams without alerting IT or the head of their business.

Cyber-safe habit #3:

Identify and report suspicious emails

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%) share passwords between team members.

Cyber-safe habit #4:

Unique logins for all team members

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

About 1 in 5 (18%) 'snooze' software updates.

Cyber-safe habit #5:

Set your devices to automatically update software

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.

Spotlight on Out-of-Office Messages

"Out-of-office" emails can be like putting up a sign that says, "Hey, I'm not here right now," particularly when you paint a picture of your travel plans. Online criminals can use this information to scam the business by impersonating the owner or employee on leave. 1 in 10 small business owners have observed personal details added to out-of-office messages.

CASE STUDY: Holiday impersonation scam

In early 2023, the owner of an Australian family-run business took a well-earned international holiday. Excited to be on leave, and to remind people they'd be out of contact their out-of-office message contained travel dates and details of the places they were looking forward to be visiting!

Using the information in the email, the cyber criminal devised a targeted impersonation attack pretending to be the CEO stuck in a specific travel location with a compelling story of having had their accounts locked overseas. Could the accountant please transfer money to a local account?

Thankfully, the business had a well-established process to double verify large transactions and was able to identify the scam at the last minute!

The lesson: Keep your out-of-office email response simple and avoid personal details.

Here's what you should remember:

1. Avoid personal details.
2. Don't share your travel destination.
3. Avoid listing your exact length of holiday.
4. Consider creating different out-of-office replies based on whether the message is going to someone inside or outside your company.
5. Consider using a general email address to refer customers to, instead of towards specific employees.

Example

Thank you for your email. I am currently away from my computer and may be delayed in my response. For urgent matters, please contact our team at [general team email] or call the office at [office phone number].

Best regards
Sarah

Cyber attacks are more common than you think

Don’t leave your business unprotected.

Cyber Wardens training helps small businesses lock their digital doors. In less than 45 minutes the free Cyber Wardens training gives quick cyber security wins to keep small businesses safe.

The top 4 best ways to protect your business

1. Defend against digital break-ins with up-to-date software

2. Set up a virtual alarm system with MFA (multi-factor authentification)

3. Password like a pro by upgrading to passphrases and password managers

4. Bounce back with backups

About the research

This research was undertaken by 89 Degrees East and conducted in November 2023. These findings are drawn from a national survey of 2,096 Australian small business owners and employees.

Profession

50% Owners

50% Employees

Gender

57% Female

42% Male

1% non-binary

Geography

72% Metro

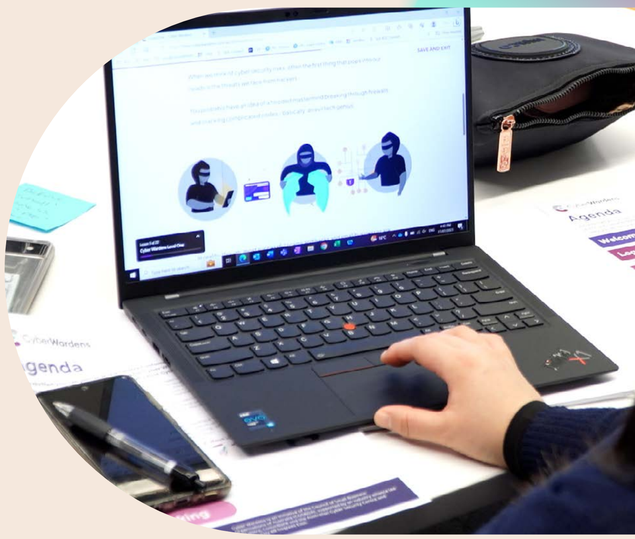
28% Regional

Age

18-24 years	6%
25-34 years	22%
35-44 years	24%
45-54 years	18%
55-64 years	18%
65+ years	13%

*adds up to 99% due to rounding

Become a Cyber Warden



Making simple swaps in the everyday habits of your business is the easiest way to kickstart your New Year's resolution to make cyber safety a priority in 2024.

Start the new year by choosing simple everyday habits to protect your business from cyber criminals.

Join our free 45-minute Cyber Wardens training. You'll learn simple, effective ways to keep your business cyber-safe.

Enrol now and make cyber safety a part of your New Year's resolution.

CyberWardens.