

Cybersecurity for Small Business update

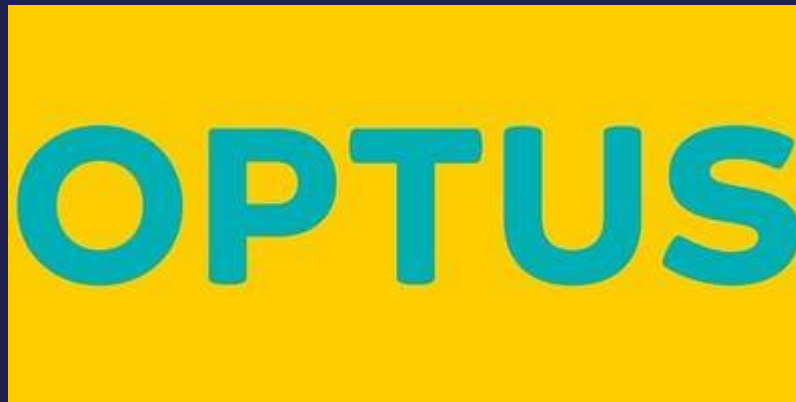


The background image features a person wearing a dark hoodie, seen from the chest up, with their hands on a laptop keyboard. The person's face is obscured by the hood. The background is a dark blue-grey color filled with vertical columns of glowing white and light blue digital code, resembling a 'Matrix' style. Interspersed among the code are several words in a bold, white, sans-serif font: 'PASSWORD', 'HACKER', 'INTERNET', 'ASSWORD', 'DATA', 'SECURITY', 'BREACH', 'IDENTITY', and 'THE'. A semi-transparent grey rectangular box is positioned in the lower center of the image, containing the main title text.

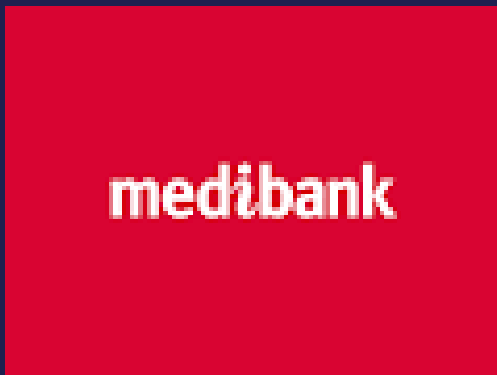
Cybersecurity Awareness session for small business



139 million



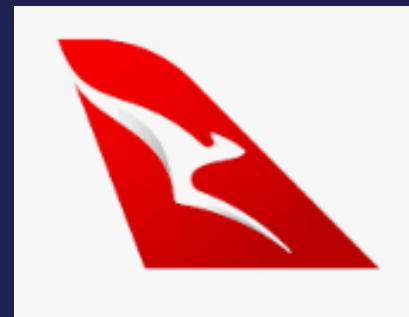
9.8 million



9.7 million



8 million



7.6 million

Exclusive: Victoria's Loyola College confirms cyber incident

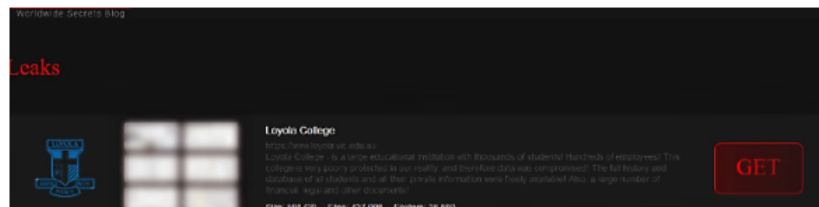
A Catholic college resets all staff, student, and parent passwords as the Interlock ransomware gang posts almost 600 gigabytes of stolen data to the dark web, including passports and financial records.



David Hollingworth • Mon, 01 Sep 2025 • **SECURITY**

SHARE

A Catholic college in the Victorian suburb of Watsonia has confirmed that it is actively investigating a cyber incident after the Interlock ransomware gang listed the school as a victim



Cybersecurity definition:

Cybersecurity is about protecting your business's digital stuff (like bookings, emails, and customer info) from online threats, scams, and data leaks.

Think of it as locking the doors to your online office, just like you would your cellar door or reception desk.

Entered into Copilot (Microsoft's AI tool):

Give a brief definition of
cybersecurity for a group of
regional tourism operators

Scam trends in Australia

Education and awareness is one of the best ways to combat scammers



Please note: Statistics provided are obtained from ScamWatch (www.scamwatch.gov.au) and attributed to the © Commonwealth of Australia

The Cyber Security Risk Landscape

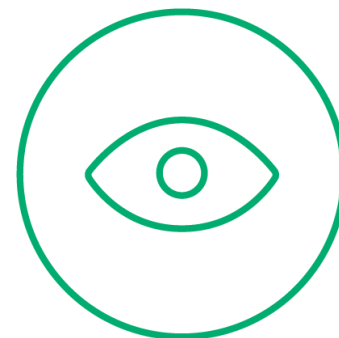


In 2023 Australians made over 601,000 scam reports compare to 507,000 in 2022 – an increase of 18.5%

This is over one report for every minute of the year



Medium businesses had the highest average financial loss per cybercrime report (**\$88,000**) compared to small businesses (**\$39,000**) and large organisations (**\$62,000**).



Fraud, online shopping and online banking were the top reported cybercrime types, accounting for **54%** of all reports.

Top 5 scams by loss



Investment

\$1.3 b



Remote access

\$256.0 m



Romance

\$201.1 m



Phishing

\$137.4 m



Payment redirection

\$91.6 m

Investment scams



What are they?

Scammers claim to have developed highly profitable trading systems based on special algorithms that deliver high returns with little or no risk. Typical scams start with a small return on investment then the scammers claim to have system problems, cut off contact and keep the money.

Investment scams were the most common scam in 2020 with Aussies losing \$328 million. More than half of reported losses in 2021 have been through bitcoin.

How to protect your business:

- Do your research. Avoid a company that doesn't have a AFS license or says they don't need one.
- Check who owns a website using websites such as who.is and check whether any account details you have been told to transfer to match the name of the company you are supposedly dealing with
- Remember if it looks too good to be true, it probably is.

Business email compromise scams



What is it?

Scammers intercept legitimate invoices, changing details to include fraudulent payment info. The recipient will pay the invoice as normal and not realise they have been scammed. Another technique is to impersonate the CEO and request staff transfer funds for reasons like surprise gift cards for staff.

Business email compromise caused the highest losses across all scam types in 2019 costing businesses \$132 million.

How to protect your business:

- Call (and speak to a trusted person) to verify ALL bank account changes.
- Educate your staff, so they're your first line of defense.
- Follow 'Scamwatch' to keep up to date.

**Almost four out of five breaches were
attributable to Organised crime**



*Verizon's 2022 Data Breach Investigations Report

Phishing scams



What are they?

‘Dodgy’ emails / SMSs designed to trick recipients out of money and data.

It’s a numbers game. Phishing emails / SMSs are typically sent to thousands of people. Also be mindful of ‘*spear phishing*’ (more targeted and sent to specific individuals – like reception or payroll staff).

How to protect your business

- Be wary of requests for money (especially if ‘urgent’ or ‘overdue’).
- Be cautious of opening attachments, or requests to confirm login details.
- Hover your mouse over hyperlinks to reveal the *real* link (it might not be what you think!).
- Forward SMSs to Telstra’s 7226 number and then delete

Malware and ransomware scams



What are they?

Malicious software (“Malware.”) is unauthorised software designed to cause harm (e.g. viruses, trojans, worms.) Ransomware is a popular type of malware that locks down your computer and files until a ransom is paid.

Malware gains access to important sensitive information (like banking details, credit card numbers, and passwords).

How to protect your business

- Automatically update your operating system, software and apps.
- Regularly backup your files – consider a copy that’s kept offline.
- Have a response plan in place. Know who to call if a ransomware attack occurs.
- Never pay a ransom! You are not guaranteed to regain access, and may be vulnerable to a second attack.

A man and a woman, both wearing white hard hats and high-visibility yellow and blue work jackets, are standing in a factory. The man, on the left, has a beard and glasses. They are both looking at a laptop held by the woman. The background is a blurred industrial environment with large machinery and bright lights.

**Ransomware increased
13% over the previous year
—a jump greater than the
last five years combined**

False billing



What is it?

False billing scams request you or your business to pay fake invoices for directory listings, advertising, domain name renewals or office supplies that you did not order.

Scammers recognise that small business operators are busy and have fewer resources than large businesses, so they aim to take advantage of that. It's easy for a scammer to copy or modify letterheads, names and logos to make them look real, or set up a professional-looking but fake website.

How to protect your business

- Never agree to any business proposal on the phone: always ask for an offer in writing
- Check that goods or services were both ordered and delivered before paying an invoice
- Get proof of directory entries before paying anything and never pay for an entry or advertisement you didn't authorise.

Cyber Security for Small Business

What else can you do?

- **Use Multi-Factor Authentication:** MFA is a security measure that requires two or more proofs to grant access to your accounts. A typical example combines something in your *head* (like a password) with something in your *hand* (like a SMS code to your phone). **Authenticator apps are better.**
- **Change to passphrases:** Try using a phrase or sentence, instead of a password. ‘Longer is stronger’, plus a sentence is easier to remember. Don’t reuse passwords across multiple sites.
- Use a **Password Manager**
- **Implement Access Controls:** Minimise risk by working out *who* can access *what* within your computing environment. Restrict admin privileges on an “as required” basis. Remember to revoke access when employees leave the business.
- **Keep informed:** <https://www.cyber.gov.au/acsc/small-and-medium-businesses>
- **Enrol in**  **CyberWardens.** <https://cyberwardens.com.au/>

Cyber Security for Small Business

We are making cyber security simple for Australian small business

The Cyber Wardens program is a simple education tool designed to build a cyber-smart small business workforce. Educating your team about cyber threats will help to protect your small business.



Cyber Security for Small Business

Passphrases..

	Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
Attempting to connect with Username: 'SYS' Password: '345'	4	Instantly	Instantly	Instantly	Instantly	Instantly
Attempting to connect with Username: 'SYS' Password: '3456'	5	Instantly	Instantly	57 minutes	2 hours	4 hours
Attempting to connect with Username: 'SYS' Password: '34567'	6	Instantly	46 minutes	2 days	6 days	2 weeks
Attempting to connect with Username: 'SYS' Password: '3456789'	7	Instantly	20 hours	4 months	1 year	2 years
Attempting to connect with Username: 'SYS' Password: '34567890'	8	Instantly	3 weeks	15 years	62 years	164 years
Attempting to connect with Username: 'SYS' Password: '4321'	9	2 hours	2 years	791 years	3k years	11k years
Attempting to connect with Username: 'SYS' Password: '43210'	10	1 day	40 years	41k years	238k years	803k years
Attempting to connect with Username: 'SYS' Password: '4567'	11	1 weeks	1k years	2m years	14m years	56m years
Attempting to connect with Username: 'SYS' Password: '456789'	12	3 months	27k years	111m years	917m years	3bn years
Attempting to connect with Username: 'SYS' Password: '4th'	13	3 years	705k years	5bn years	56bn years	275bn years
Attempting to connect with Username: 'SYS' Password: '5432'	14	28 years	18m years	300bn years	3tn years	19tn years
Attempting to connect with Username: 'SYS' Password: '543210'	15	284 years	477m years	15tn years	218tn years	1qd years
Attempting to connect with Username: 'SYS' Password: '567'	16	2k years	12bn years	812tn years	13qd years	94qd years
Attempting to connect with Username: 'SYS' Password: '56789'	17	28k years	322bn years	42qd years	840qd years	6qn years
Attempting to connect with Username: 'SYS' Password: '567890'	18	284k years	8tn years	2qn years	52qn years	463qn years

How to protect yourself from scams

Keep your personal details and financial information safe:



Do not share your financial information (i.e. bank, credit card or gift card details) or personal details with an unsolicited caller or door knockers trying to seek payment for a service over the **nbn**[™] network.



If in doubt, hang up and call your retail service provider on their official customer service centre number to check if the call is legitimate. Do not use contact details supplied by the caller.

If you think you've given your details to a scammer:

- Contact your bank or financial institution straight away.
- Report it to your local police and to Scamwatch.
- Contact IDCARE on 1800 595 160 if you think you've given remote access to your computer or mobile device or revealed personal or financial information.

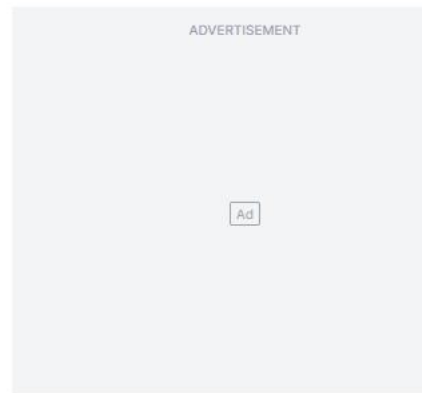
'It was just so frightening': Local residents targeted by NBN scam



By [Sophia Baker](#)

Updated May 10 2024 - 4:34pm, first published May 8 2024 - 2:00pm

0 Comments



Graeme Uebergang almost lost \$10,000 to a sophisticated scam. Picture by Anthony Brady

What to expect from nbn

We do not sell phone or internet services directly to the public

- **nbn** will never call you with automated assistance (e.g. “robo call”) to tell you you’ll be disconnected.
- **nbn** will never ask for remote access to your computer via the installation of programs.
- **nbn** is a wholesaler and will never ask you to buy a plan directly from them.
- There are times when **nbn** may contact you directly, but never to ask for payment.
- All **nbn**[™] approved technicians and workers carry enAble[™] identification cards. If you’re unsure, ask to see this.

**Most breaches,
82%, involve a
Human
Element**



*Verizon's 2022 Data Breach Investigations Report

The future is scary:

Chat GPT

Dec. 2022:	1 million users
May 2024:	180 million users
Aug. 2025:	5.3 billion visits

AI-generated voice scams have arrived

Scammers can impersonate your loved ones.

By Casey Tonkin on Mar 07 2023 10:54 AM

Print article

Tweet

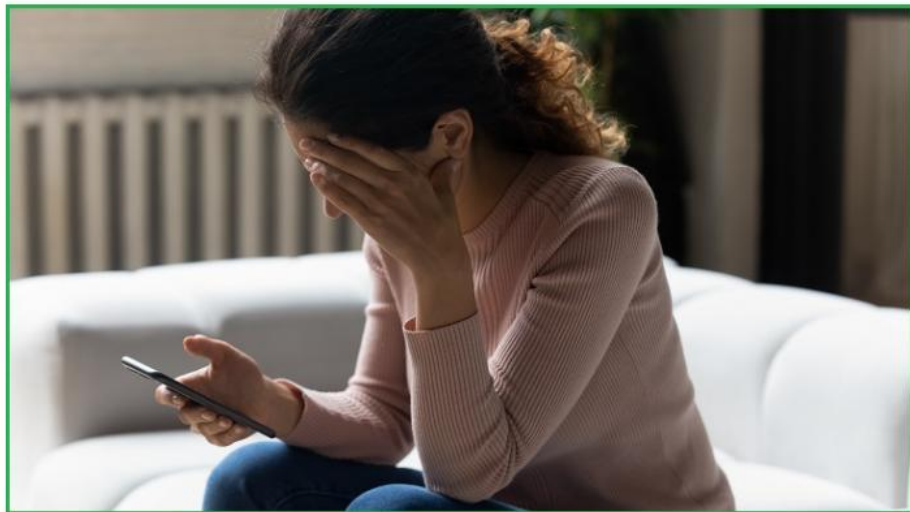
Share 110

Share

Scammers in North America have started using artificial intelligence (AI) to generate voices of people's loved ones to trick them into handing over cash – and there are concerns this technique could soon target Australians.

A story in *the Washington Post* this week outlined how the scam can be surprisingly elaborate.

That was the case with the parents of 39-year-old Benjamin Perkin who got a call from someone claiming to be a lawyer.



Helpful links

Protect yourself from **nbn scams**
www.nbn.com.au/scamadvice

Learn more about **scams**
www.scamwatch.gov.au

Report a **scam**
www.scamwatch.gov.au/report-a-scam

Try the **Digital Readiness Assessment Tool**
www.business.gov.au/online

Join the ACSC Alert Service for up-to-date
information on online threats.
www.cyber.gov.au

<https://haveibeenpwned.com/>
Great tool to discover if your email or mobile
has been compromised.

Cyber Security Awareness Month

Set up and perform regular backups

Why it matters: Backups protect your data from loss caused by ransomware, theft, or hardware failure. Without them, you could lose important files permanently.

What to do: Set up automatic backups through your system or application settings. Store a copy offline or in the cloud so you can quickly recover your files if needed.

Tip: Schedule backups to run automatically each week to keep them current without manual effort.

Keep your software and devices up to date

Why it matters: Updates are one of the strongest defences against cyber threats. They fix known vulnerabilities and improve performance and security.

What to do: Turn on automatic updates wherever possible so that your system, apps, and devices stay protected.

Tip: Cybercriminals often exploit known weaknesses in outdated software - so staying updated is one of the simplest ways to stay secure.

Use a unique and strong passphrase for every account

Why it matters: Weak or reused passwords make it easy for attackers to access multiple accounts at once.

What to do: Create passphrases that are:

- Long: at least 15 characters
- Unique: never reuse a passphrase

Password managers can help you create, store, and manage strong credentials safely.

Tip: Combine your strong passphrase with multi-factor authentication (MFA) wherever possible for maximum protection.

Turn on multi-factor authentication (MFA)

Why it matters: MFA adds a second layer of security, so even if your password is stolen, your account remains protected.

What to do: Enable MFA on all important accounts- especially email, banking, and social media. MFA usually combines:

- Something you know (password or PIN)
- Something you have (security key or phone)
- Something you are (fingerprint or facial recognition)

Tip: Use an authenticator app rather than SMS codes when possible- it's more secure.

Review your privacy and location settings

Why it matters: Oversharing makes it easier for criminals to target you.

What to do:

- Adjust privacy settings so only trusted people can see your information.
- Turn off location sharing and geotagging when not needed.
- Limit app permissions such as photo or camera access to only what's necessary.

Tip: Review settings after every major app update, as new permissions may be enabled automatically.

Be cautious when using public Wi-Fi

Why it matters: Public Wi-Fi in cafes, hotels, or airports is often unencrypted, making it easy for attackers to intercept your data.

What to do:

- Avoid logging into banking, email, or social media accounts over public Wi-Fi.
- Use your mobile hotspot or a trusted VPN when you need to connect securely.

Tip: Always turn off automatic Wi-Fi connections to prevent joining insecure networks without realising it.

Be alert for scams and phishing

Why it matters: Scams and phishing emails try to trick you into revealing personal or financial information.

What to do:

- Think before you click—avoid links or attachments from unknown senders.
- Verify unexpected messages directly with the organisation.
- Watch for red flags like urgency, errors, or requests for sensitive data.

Tip: Report suspicious emails using the 'Report Phish' button.

Get involved in Security across your team

Why it matters: Security Champions help create a strong security culture by making good habits part of everyday work.

What to do:

- Join the 'Security and Privacy' and 'Scamfit' groups on Viva
- Share tips and promote awareness in your team.
- Support phishing drills, training, and security initiatives.

Tip: Small actions - like engaging with our Viva content can make a big difference.

Thank you Questions...