

Cybersecurity for small and medium business

Stay safe in today's business environment



Keeping your business cybersafe

Do you lock your door at night? Your car, when you go to the supermarket? Do you make sure your work space is locked up and secure at the end of the day?



Safeguard your people, data, and infrastructure

We all take security measures in life, but many small and medium businesses say they don't feel equipped to manage their businesses' cybersecurity needs. In reality, cybersecurity is just as important as physical security, and cyber threats are only getting more sophisticated.

Unfortunately, cybersecurity attacks are the new normal for businesses, however – you are not alone and Microsoft is here to help.

In this eBook you'll learn about the cybersecurity landscape, about the different cybersecurity threats, how to spot them and what you can do to protect your business.





Contents

01

What are you protecting?

- 04 What are you protecting?

02

Cybersecurity threats

- 05 Cybersecurity threats
- 06 Phishing
- 07 How to avoid becoming a phishing victim
- 08 Network attacks
- 09 Malware
- 10 Ransomware
- 11 Tech scams

03

Harness your people power

- 12 Harness your people power
- 13 10 ways to protect your employees and your business

04

Cybersecurity cheat sheet

- 14 Cybersecurity cheat sheet

05

Employee guide

- 15 10 easy rules to secure your personal data & protect your devices

What are you protecting?

Q: What have you got to lose?

A: Everything

Q: What have you got to protect?

A: Also everything

Often when it comes to areas outside of our expertise like IT, it can seem impossible to understand the problem, let alone manage issues that arise. But what is the cost of keeping your head in the sand? And what does that cost translate to if you have an attack without any protection? So, what do you need to protect?

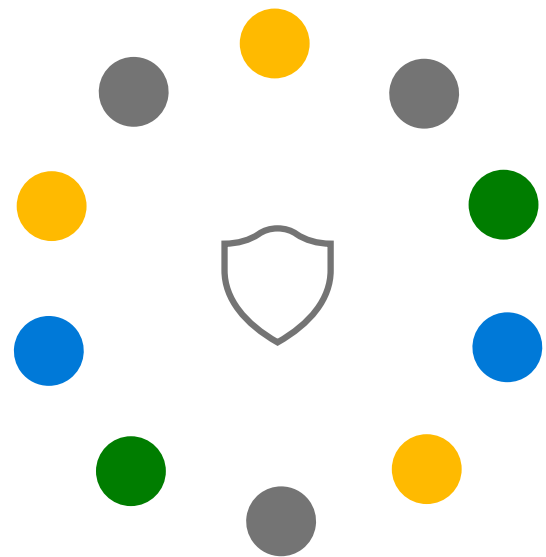
Your data

In the modern world, your business data is one of your biggest assets; customer details and information, financial and payment details, your business records – all of this is key to keeping your business operational and compliant. Your data is also a very attractive proposition to criminals looking for a quick way to make money – using or selling these details can be lucrative for these criminals.

Your reputation

When people and organisations do business with you, in a way, they're saying *'I trust you with my data'*. If you have gaps in your security protection, that means you are a target for cybercrime, and that trust can be lost.

For most businesses, a loss of trust carries a high price – consider the leak of more than 400,000



Australian bank card details¹, or imagine you're a customer of an organisation mentioned in an increasing number of cyber attack news reports and stories.

Your business

Our ability to operate outside the digital world is almost impossible, so an interruption to your organisation's online services can result in the loss of revenue, time and hits your company's bottom line. One report even suggests that [60% of small businesses fold](#) within six months of a cyber attack.² Whether it's via a [phishing](#), [malware](#) or a [network attack](#), cyber threats are a real risk to your business that could result in your business closing its doors; and so critically, we want to avoid this happening to you.

What can you do?

Read on! By taking the right steps to secure your business, you can lock down your systems the same way you lock your doors at the end of the day. It doesn't mean nothing can happen, but it's much easier to break into an open house than a locked one.

¹Source: Shocking number of Aussie payment cards on dark web – Sarah Sharples, news.com.au, 2 December 2021

²Source: 60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack – Joe Galvin, Inc, 7 May 2018

Cybersecurity threats

What is cybersecurity?

Cybersecurity, also known as computer security or information technology security, is the protection of computer systems, including hardware, software and networks from cyber attacks.

Why do small and medium businesses need cybersecurity?

Cybercrime is on the rise and cybersecurity threats can do real damage to business; they can shut down your operations, steal your sensitive data, and hold you to ransom.

Unfortunately, small and medium businesses are just as susceptible to cybercrime as large enterprises, so it's important to make sure you have the right protection in place for your business.

Cybersecurity threats: *know what you're up against*

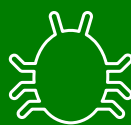
You don't know what you don't know, so here we explore the most common types of cybersecurity threats, how to spot them and what you can do about them.



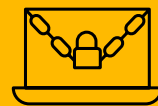
Phishing



Network attacks



Malware



Ransomware



Tech scams

Phishing

(aka social engineering attacks)

What is it?

Email and text messages that try to trick you into clicking on a malicious link that allows hackers to gain access to your systems or gets you to provide sensitive financial and personal data. Criminals use the data for identity theft or resale.

What to look for

- A trusted sender, such as your bank, a government department, a large organisation
- An urgent request
- A link or attachment; something you need to click on like a link to a website, or an attached file.

What not to do

If you think it's a phishing threat but you're not sure, the best action is **inaction** – don't do what they want (don't click the link, reply to the email, supply sensitive details).



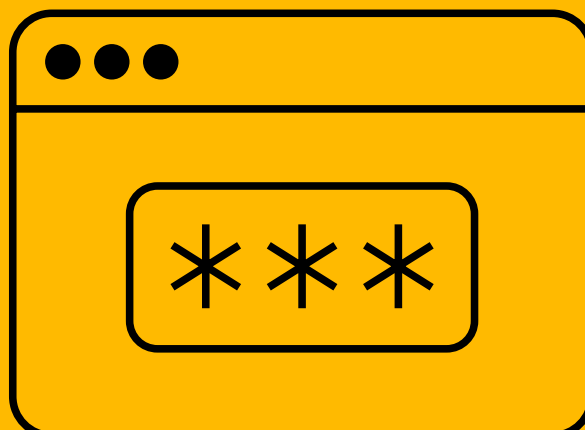
What to do

- Contact the organisation or person in a different way from the request (call them, for example) using information you have already or can find online, and ask them directly if they sent the message
- Send an email to the organisation or person directly, or
- Go to the official website, log in and respond that way.

Did you know...?

There is more than one way to phish:

- **Vishing:** Like phishing, but using phone calls.
- **Baiting:** When the attacker offers a fake prize for responding.
- **Browser attacks:** May appear as pop-up ads or suggestions to install a browser extension.



How to avoid becoming a phishing victim

1 Inspect the sender's email address closely. Look for small changes signaling a fake identity.

Be wary of emails that utilise a generic greeting, asking you to act urgently.

2

3 Look for verifiable sender contact information. If in doubt, do not reply. Start a new email to respond.

Use the phone to convey private information. Never send sensitive information via email.

4

5 Avoid clicking on unexpected links. Go to the official website and log in instead.

Avoid opening email attachments from unknown senders or even friends who do not normally send you attachments.

6



7 Install a phishing filter for your email client. Use the spam filter on your email account.

Network attacks

(Denial of Service or 'DoS')

What are they?

Network attacks overload your system, server, or network with traffic, so you can't access the systems you need to run your business. There are also 'Distributed denial of service' (DDoS) attacks, which use multiple computers in several locations.

	Denial of service (DoS)—An attack where a computer sends many requests to a network service to overwhelm the target service.
	Distributed denial of service (DDoS)—A DoS attack using multiple computers in several locations.



What to look for

Network attacks can be tricky to identify for non-IT people, but some of the hallmarks of a DoS or DDoS include:

- Unavailability of a specific website
- Unable to access any website at all
- Unusually slow network performance – can't open a file or website.

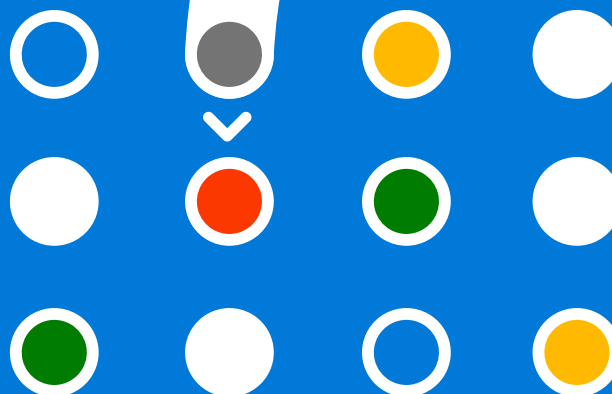
What to do

- To confirm you are experiencing a network attack, contact your internet provider or IT support organisation
- If a network attack has occurred, initiate your IT disaster recovery plan.

Prevention is the cure

Azure DDoS Protection Standard helps defend against DDoS attacks; it is automatically tuned to protect all public IP addresses in virtual networks.

[LEARN MORE](#)



Malicious Software

(Malware)

What is it?

Malware is malicious software; what used to be called a 'virus'. Malware can steal your personal or business data, use your hardware as a base from which to quietly attack other machines, or any number of other malicious tasks.

What to look for

Similar to phishing; look out for emails or communications that don't seem quite right, that ask you to take an urgent action.

What to do

- Be careful (see recommendations under ['Phishing'](#))
- Make sure your operating system and applications are updated with the latest security patches
- Be defended – have an active, current, anti-malware program running on your computer. Windows 11 includes Microsoft Defender Antivirus which runs by default.



Ransomware

What is it?

Ransomware is type of malware that locks down your computer or files until a ransom is paid. Imagine you log in and all your customer data, all your digital assets and information is gone; how do you do business?

What to look for

Ransomware works by encrypting or locking all of your files, programs, databases, documents, photos and videos. A pop-up window typically then appears, demanding money is paid in exchange for an encryption key, which will unlock your files.

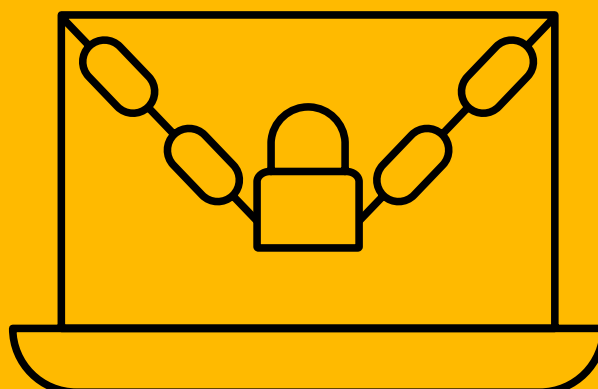
What to do

- Make sure you have a secure back up of your important business data.
- Make sure your software, systems and apps are all automatically updated.
- Protect your access with passwords and authentication processes.
- Ask a professional to do a security audit to see if there are gaps in your defences.



Reporting ransomware

The Australian Cybersecurity Centre (ACSC) recommends you never pay a ransom. If you experience a ransomware incident and require support, call the ACSC's 24/7 hotline on 1300 CYBER1 (1300 292 371).



Tech scams

What are they?

Tech support scams are common; they are where scammers try to get you to pay them to 'fix' a nonexistent problem with your device or software. While some may want money, others want to steal your personal or financial data or may even try to destroy your personal or company network and demand you pay a ransom.

What to look for

6 pro tips to protect yourself from tech support scams:

What to do

- If you've experienced a tech support scam:
- Uninstall any applications scammers have asked you to install.
- Run a full scan with Windows Security to remove any malware.
- If you have given scammers access to your computer, reset your device.
- Change your passwords.
- If you have already paid, call your credit card provider as soon as possible.
- Report unsafe websites in Microsoft Edge by going to Settings and More > Help and Feedback > Report unsafe site.
- Report tech support scams:



www.microsoft.com/reportascam

1 Clue Someone claiming to be tech support calls you.	Pro tip Microsoft never makes unsolicited phone calls. If you didn't reach out to us, we won't call you to offer tech support. Be aware, scammers often fake Caller ID.
2 Clue You get an error message asking you to call a number urgently.	Pro tip Microsoft error messages never include phone numbers. The Microsoft Edge browser blocks known support scam sites using Microsoft Defender SmartScreen.
3 Clue Tech support asks you to pay them to fix your 'problems' with cryptocurrency or gift cards.	Pro tip If you've requested tech support, they'll tell you ahead of time if there's going to be a fee, and that fee will never be in the form of cryptocurrency like Bitcoin or gift cards.
4 Clue Tech support asks you to download software from an email or third party website.	Pro tip Download software only from official websites, Microsoft partners, or the Microsoft Store. On your mobile devices, only download from the official app store.
5 Clue Tech support asks you for your password or other private, sensitive data.	Pro tip Microsoft tech support never asks for your password, social security number, or other personal data.
6 Clue You are asked to share your screen via 3rd party app to help resolve an issue with your computer, giving full access to the scammer to all your files.	Pro tip Never share your screen unless you are sure it's a trusted source.

Harness your people power

One thing people often underestimate is the power of people when protecting your business.

Training and empowering employees – all employees – can help safeguard your business from a cybersecurity attack. So, what can you do?

Start at the very beginning:

Make sure cybersecurity measures and a discussion about any IT policies and processes are a part of your onboarding.

Be strategic:

Map out which roles have access to systems, and ensure you remove or update users and accounts once they leave or change roles.

Consistency is key:

Enforce [corporate file saving protocols](#). Store and encrypt company data securely in the cloud.

Make sure you have an IT disaster recovery plan

An IT disaster recovery plan aims to identify steps you need to take to assess damages and restart operations. It should also determine who's responsible for which tasks and specify how often to review and update the plan.

Build security into your company's DNA

By making cybersecurity part of your organisational culture, you're both protecting your business and teaching your staff important skills that apply to life as well as work.

Engage to empower:

Raise employee awareness of potential risks when online; provide your employees engaging with training and update your training procedures as you roll out new policies or procedures.

Automate:

Implement automatic password update and software update processes.

Have a plan for devices:

You and employees are likely accessing business data from multiple devices. While it's very convenient to check work emails on your phone, that also opens up a potential vulnerability. Be sure you're incorporating [mobile device security](#) into your cybersecurity plans.

If you're not sure where to start with an IT disaster recovery plan, it may be worth contacting a reputable IT support provider for assistance.

10 ways to protect your employees and your business

1 Provide your employees with training on safe email and browsing use.



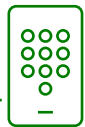
2 Raise employee awareness of potential risks when online.



3 Offer your employees attack simulation training in Microsoft Defender for Office 365.



4 Go passwordless and use multi-factor authentication.



5 Ensure all company devices use the latest version of Windows and internet browser.



6 Enforce corporate file saving protocols. Store and encrypt company data securely in the cloud.



7 Educate employees on the importance of using secure connections such as HTTPS. Install the HTTPS Everywhere plug-in for your browser.



8 Make it a practice with employees to check website certificates to verify the identity of the website.



9 Enable pop-up blockers by default.



10 Use cloud-based antivirus solutions like Microsoft Windows Defender.



Have a plan for devices

You and employees are likely accessing business data from multiple devices. While it's convenient to check work emails on your phone, that also opens up a potential vulnerability. Be sure you're incorporating mobile device security into your cybersecurity plans.



Cybersecurity cheat sheet

In the short term

- Make sure your software, systems and apps are all automatically updated.
- Enable pop-up blockers by default.
- Install the HTTPS Everywhere plug-in for your browser.
- Ensure all company devices use the latest version of Windows and internet browser.
- Use cloud-based antivirus solutions like Microsoft Windows Defender.
- Ensure your operating system and applications are updated with the latest security patches.

In the long term

- Make sure you have the right tools – look for products and services with a track record of success in the security and privacy space.
- Consider an IT asset strategy that ensures you're using hardware that is capable of keeping up with modern threats.

Follow best practices for passwords

It's prudent to make all passwords strong and unique. Additionally, use different passwords for different accounts. Make using strong random passwords containing letters, numbers, symbols and special characters mandatory.

Good passwords shouldn't be easy to remember. Also, prompt your staff to change all passwords every few months.

In the medium term

- Review your IT processes, procedures and training plans to make sure they are current.
- Create or update your IT disaster recovery plan – if you can, engage a quality IT consultant to test systems that have external access, such as websites, drives and folders.
- Create procedures to follow in case of a breach and make network and computer security top priorities, on par with other key business priorities.
- Make sure you have a secure back up of your important business data.



Employee guide

10 easy rules to secure your personal data & protect your devices

Here are 10 easy rules to keep your email, accounts, and devices safer and avoid identity theft.

1

Share your personal information in real time only, preferably in person or by phone. Be careful of what you share on social media.

Share personal info in person or by phone. If you absolutely must email personal information, use Microsoft Outlook's encryption tools. Protect yourself from social media hackers. Before you post to social media, think about the information that can be harvested from it.



2

Be skeptical of messages with links, especially those asking for personal information.

Find a phone number on the sender's official website and call them directly to confirm the message is legit.



3

Be on guard against messages with attached files.

Never open unexpected attachments, even if they seem to come from people or organisations you trust. If you're concerned that the message may be important, call the sender to verify.



4

Go passwordless and use an authenticator app for stronger security.

They can't steal your password if you don't use one. Turn on passwordless for your Microsoft account to sign in with your phone or Windows Hello instead.



5

If you must use passwords, make them strong and unique with a password manager.

Strong passwords have at least 14 random characters and symbols. Use [Microsoft Edge](#) to remember passwords and manage password changes.





6

Enable the lock feature on all your mobile devices.

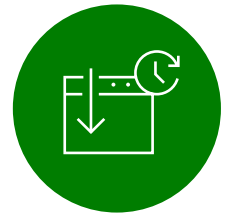
Require a PIN, fingerprint, or facial recognition to unlock your device.



7

Install software updates immediately.

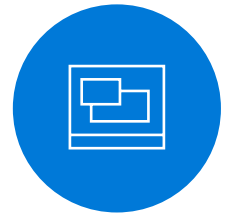
Many app and operating system updates are security fixes for currently active issues, so install them promptly.



8

Ensure all the apps on your device are legitimate.

Only install apps from the official app store for your device.



9

Use Windows 11 and turn on Tamper Protection to protect your security settings.

Always use the latest version of Windows. Tamper Protection blocks unauthorised changes to your security settings.



10

Keep your browser updated, browse in incognito mode, and enable Pop-Up Blocker.

Install browser and operating system updates immediately to maintain the latest security standards.





Learn more about Cybersecurity
for small and medium business

[https://www.microsoft.com/
en-au/security/business](https://www.microsoft.com/en-au/security/business)