myBUSINESS

Cyber security:
Helping your business stay safe online

Contents

Safeguarding your business

As more Australian companies conduct a majority of their business online, cyber criminals are becoming smarter and better resourced. If successful, this can cause significant disruption to an organisation – by stealing classified information or funds. So, if you're running a business, cyber security has never been more important.

In a way, it's a lot like taking out insurance to shield your business from things like theft and product liability. Implementing cyber security measures can help safeguard your technology and information from cybercrime, and support your recovery should your business experience a cyber attack.

This cyber security guide was developed to help you understand cybercrime, the risks it poses and the steps you can take to navigate potential threats and protect your business.

Cyber crime
a real-life threat

How serious is cybercrime?

Cybercriminals use computers and the scope of the internet to break the law. It's a very serious threat – even if it doesn't always feel very tangible. In fact, it's estimated that cybercrime costs Australian businesses a whopping $29 billion each year.

While some acts of cybercrime are classified as scams, an ACCC report found Australians lost over $850 million to scams in 2020 with business email compromise costing Australians $128 million. These figures are expected to increase as we continue to share and collect more information online.

Cybercriminals can employ an array of frightening strategies, including holding data to ransom, encrypting data so it is inaccessible, stealing funds from bank accounts, theft of personal or classified information and even of whole identities. Not only can this damage a business's bottom line, but it can also have flow-on effects for your customers.

Smaller businesses tend to be especially vulnerable, often because they don't see themselves as a target. And while many are experts in their field, without a dedicated IT professional, there is often a skills shortage to mitigate cyber threats or respond appropriately when they occur.

How cybercrime can affect your business

What’s at risk?

Cybercrime often manifests as identity theft and fraud, online scams and attacks on your business’s computer systems or website. And there’s a lot at stake. Things at risk include:

- customer records
- business plans
- financial records
- intellectual property
- employee records

Cybercrime isn’t only committed by garden variety criminals out for financial gain, sometimes, clients, competitors and current or former employers also commit cybercrimes.

Here are some of the most common types of cybercrime

Phishing

Phishing are malicious messages that try to trick you into providing private information about your business. They usually include a link to click or an attachment to open, followed by a request to share information. According to the Australian Cyber Security Centre, online banking logins, credit card details, business login credentials and passwords are some of the most common targets.

Messages are often sent via email, (phishing), SMS (smishing), social media and even over the phone (vishing). SpearPhishing is a targeted attack against an individual, small group, or individual business. Usually tailored to a common interest of that user or group. They can look very real, and may even feature a company logo, branding and links to authentic-looking websites. They're sent hoping to catch you out — perhaps you're waiting for a delivery or have a bill due.

Business email compromise

Business Email Compromise (BEC) is when a hacker gains unauthorised access to a user's mailbox and then uses that mailbox to defraud the company, clients or suppliers, extract sensitive information, or utilise the mailbox to access credentials for further BEC attacks.

According to the ACCC's annual Targeting Scams report, $128 million was lost to BEC in 2020. Scamwatch alone received around 1,300 reports, up from 900 in 2019.

Note

To help protect yourself, always check the URLs if the email contains a link. It's good practice to verify payment requests by calling or discussing in person to ascertain the request is genuine.

Malware

Malware, or ‘malicious software’, is typically used to steal information, your computer’s resources or money. It can be spread by:

- viruses
- trojans
- worms
- spyware

These are usually distributed through emails, fake websites, pop-up ads and infected files. Once clicked, they install themselves onto your computer, which gives cybercriminals access to your files and/or system. With that, you give them the opportunity to use your credit card details or copy your client database.

Ransomware

Ransomware is a type of malware that infects computers connected to the internet or a corporate network. Once a device becomes infected with ransomware it encrypts all the files on that device and can spread throughout the network the computer is connected to, rendering it unusable unless you pay a fee, or 'ransom' or restore the files from backup. The ransomware is spread through malicious websites, email attachments, social media messages and apps.

Note

Paying a ransom doesn't guarantee the attackers will fix your computer or restore your files. In fact, it could end up making you a target for further attacks.

Hacking

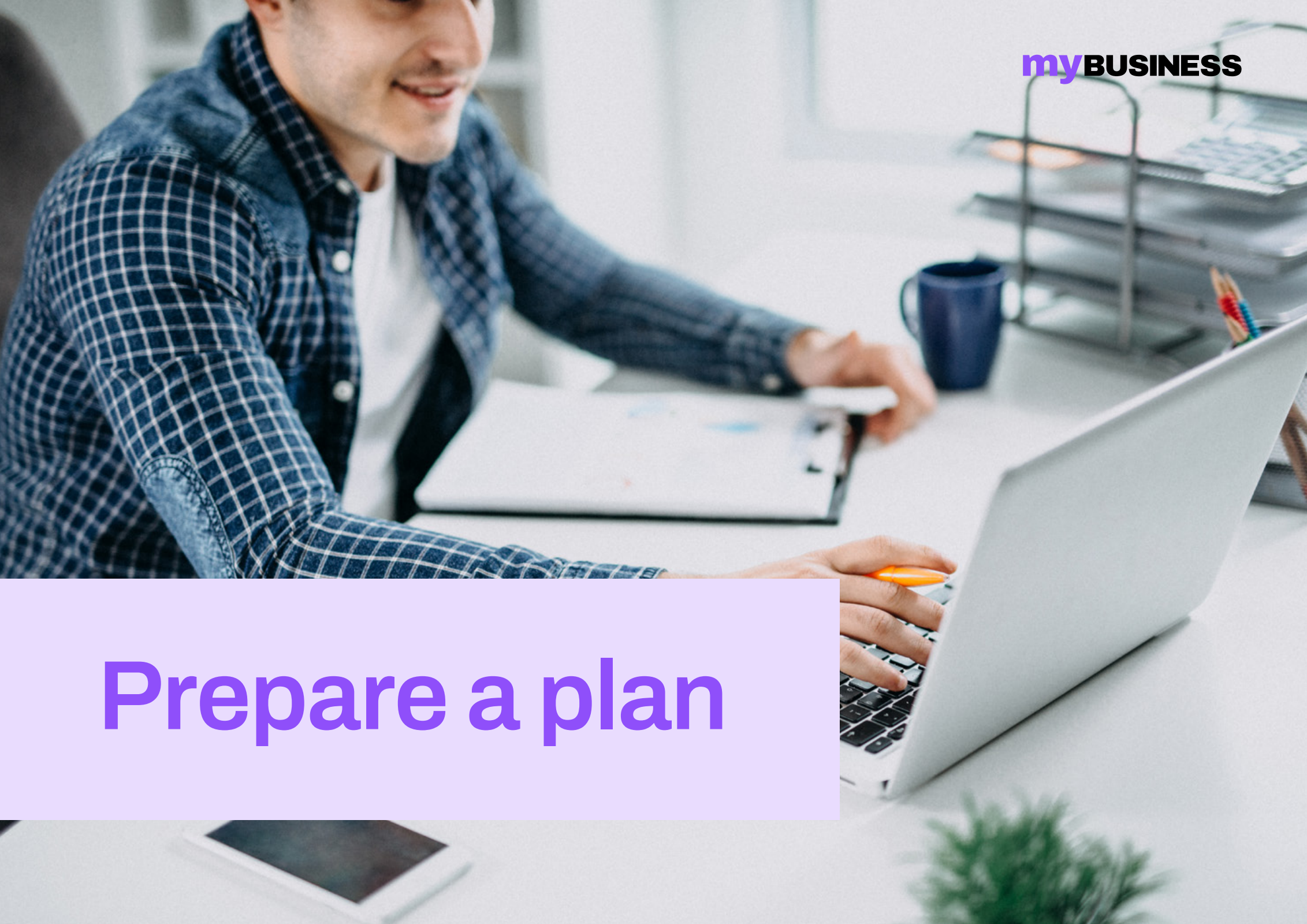
It might sound like its comes straight from a science fiction movie, but hacking is a very real problem. Using hacking software/tools, hackers can gain access to your network and wreak havoc by modifying how your network works, stealing data, obtaining and changing passwords, creating network accounts with administration privileges, retrieving credit card information and installing malware.

Website vandalism

Website vandalism can be particularly troublesome for smaller businesses. It's when the content of your website is changed without your approval. Sometimes hackers want to cause trouble and inject malicious code into websites.

Motivations can also be political – this is when hackers vandalise websites with electronic 'graffiti'. Visitors to your website can also become victims themselves when they download something the malicious actor has uploaded that ends up infecting their computer.

myBUSINESS



Prepare a plan

Developing a cyber security incident response plan

Being prepared is your best defence against cybercrime. The most effective way to limit and respond to a cyber security incident is having a cyber security incident response plan in place. Having these processes in place for everyone to see can help reduce potential damage and get you back up to speed sooner.

Generally, a comprehensive plan should include:

Cyber risk assessment including the likelihood and severity of potential cyber security incidents. What sorts of threats are unique to your industry? What sort of data do you store? Who do you do business with?

Identification of key assets, data and critical systems. What do you need to protect and why?

Plans for dealing with each type of cybercrime including phishing, malware, ransomware, hacking and website vandalism. Include time frames and objectives.

Division of key roles and responsibilities among management staff. Who does what and who do they report to? Who can make decisions?

Key tools including contact lists and guides for use during the response.

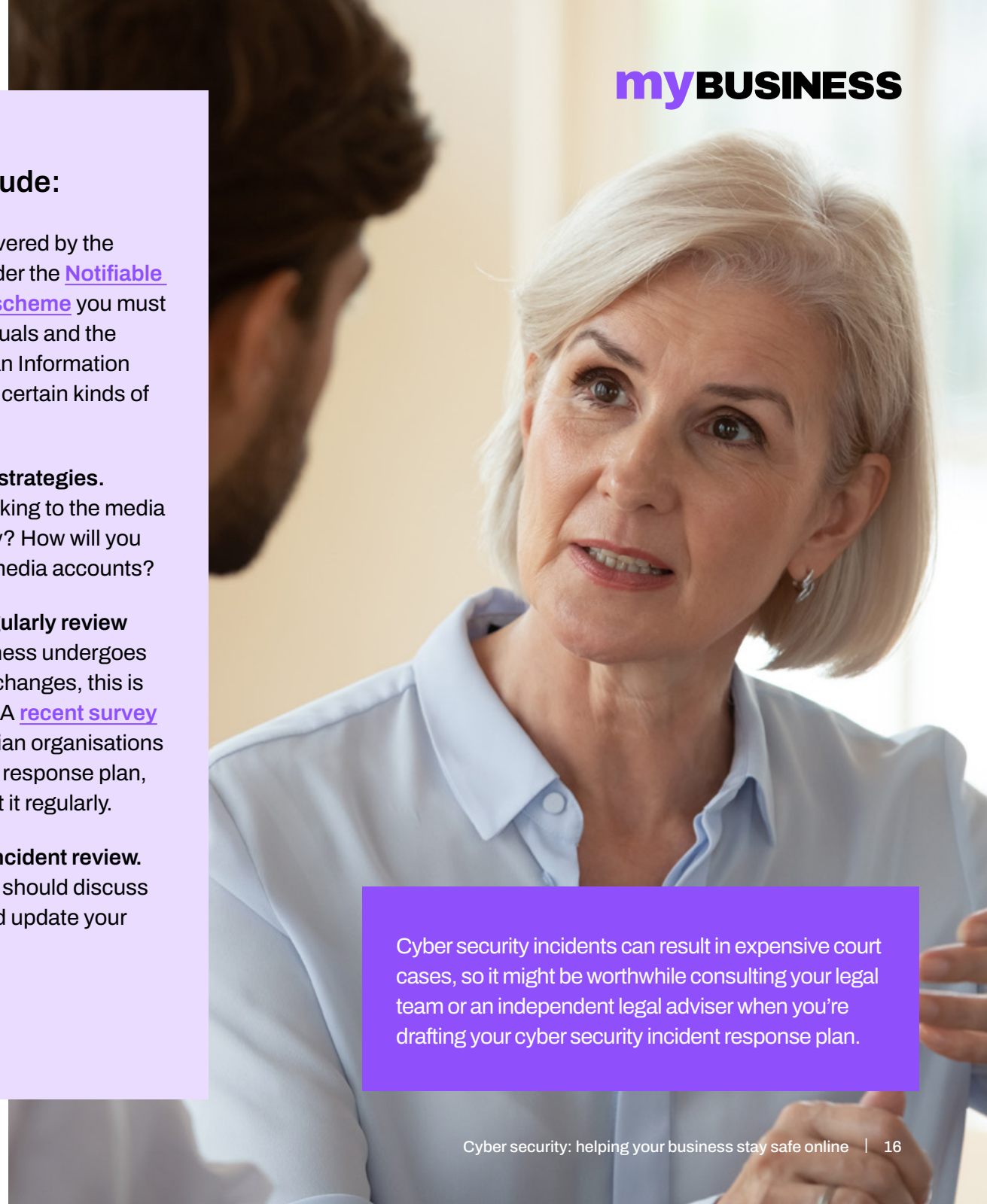
Process for alerting stakeholders including suppliers and external agencies.

If your business is covered by the Privacy Act 1988, under the Notifiable Data Breach (NDB) scheme you must notify affected individuals and the Office of the Australian Information Commissioner about certain kinds of data breaches.

Media management strategies. Who's in charge of talking to the media and what will they say? How will you manage your social media accounts?

Arrangements to regularly review the plan. If your business undergoes significant growth or changes, this is especially important. A recent survey found 54% of Australian organisations have a cyber incident response plan, but only one-third test it regularly.

Strategies for post-incident review. After an incident, you should discuss the lessons learnt and update your plan accordingly.



Cyber security incidents can result in expensive court cases, so it might be worthwhile consulting your legal team or an independent legal adviser when you're drafting your cyber security incident response plan.

Cyber security measures for your business

myBUSINESS

Protect your business

All of this may sound a little worrying right now, but the good news is there are lots of simple, practical cyber security solutions you can introduce to protect your business from potential threats.

Implementing the right measures

First things first, have a system for regular backups. This helps you recover what's lost in the event of an attack. Be sure to back up everything that's important to your business, including customer records, business plans and financial records. Ensure the backups are kept offline so they don't get infected and you test the restore process to ensure you can recover.

Next, protect your data by installing anti-virus, anti-spyware, anti-spam filters and firewall security on all of your devices. It's also best to enable automatically updates, so you always have the latest version running.

You should also consider encrypting data (converting data into a secret code) when it's at rest or being transmitted. This way, only approved users can access it.

Change passwords to passphrases (a sequence of words). Use separate passphrases for different accounts/services and where possible use Multi-Factor Authentication (MFA). After all, 80% of data breaches involve weak or stolen passwords. If you're struggling to keep up, use a password management tool like LastPass to safely store and create passphrases for you. When it comes to phishing emails, spam filters help reduce the amount of suspicious email traffic you receive.

It's especially important to keep your customer database safe and to comply with data regulations as there can be legal consequences for exposing their Personal identifiable information (PII). Provide a safe online environment for transactions and secure any personal information that you plan to store.

Tip | While it can't protect your business from cybercrime, cyber insurance can protect you from financial losses.

Develop a cyber security policy

A cyber security policy informs employees and other stakeholders of their responsibilities to protect your business's technology and digital assets. It's similar to policies you'd already have in place for things like health and safety, leave requirements or harassment. Just like those, your cyber security policy should be embedded into your company framework and provided to all you employees.

Your cyber security policy could include guidelines on:

- **Password requirements** e.g. when to update passwords and how to store them correctly
- **Email standards** e.g. when it's appropriate to share a work email address and how to report suspicious emails
- **Handling of sensitive data** e.g. what staff can and can't share
- **Locking computers and devices** e.g. when to lock screens and shut down devices
- **Handling of removable devices and technology** e.g. where staff can access technology away from your office and how to report a theft
- **Social media and internet access standards** e.g. what's appropriate to share on social media and which platforms can be accessed with a work email account
- **The role of staff** in the cyber security incident response plan.

myBUSINESS

Your employees are your best **defense against a cyber attack.**

Train your employees to spot scams like a boss with our cyber security training software for businesses. My Business Cyber includes automated staff training, phishing simulations, tools and resources.

Find out more