more
than
money

Cyber Security Toolkit

Smart strategies to safeguard your business

NAB Secure

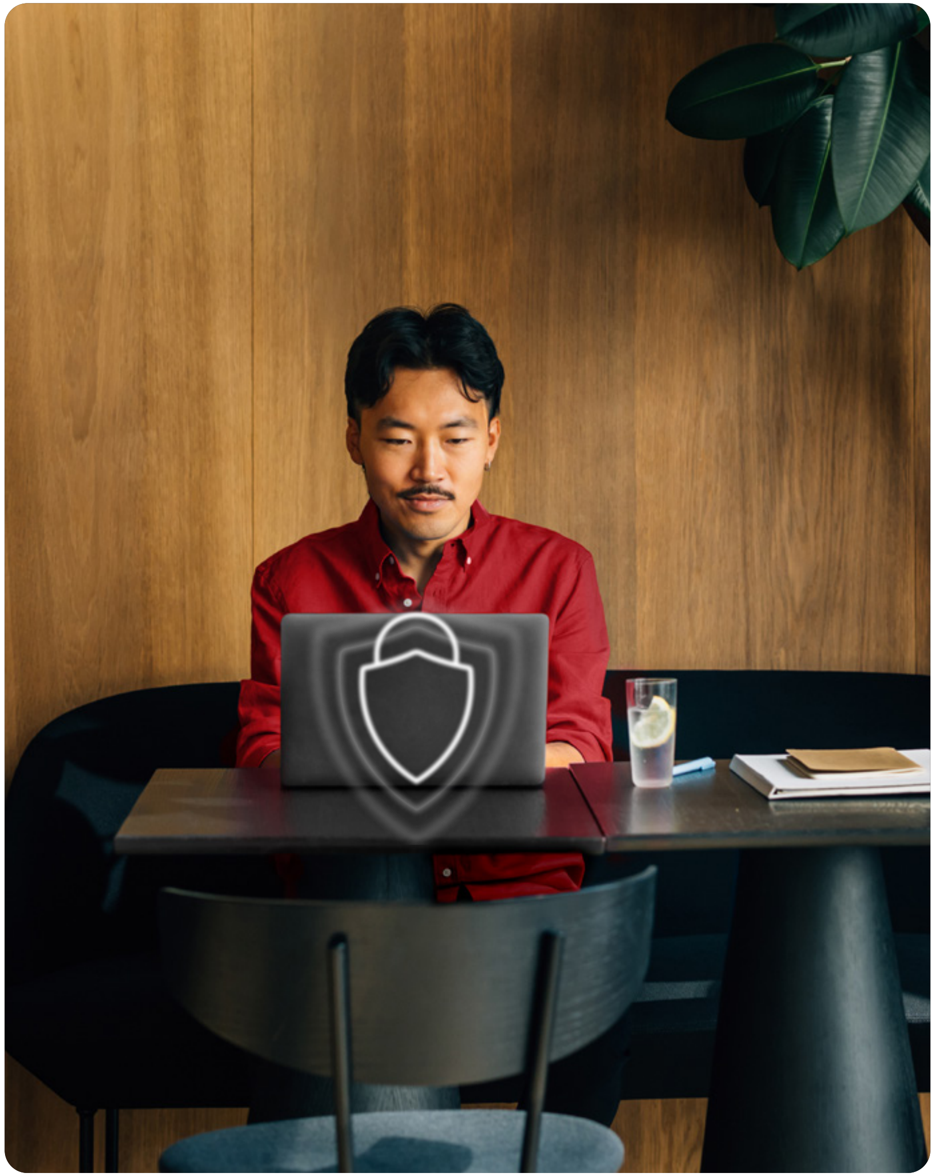
Why cyber security matters for your business

NAB Group Economics research shows around 3 in 10 Australian small and medium-sized businesses have experienced a cyber attack or data breach during the life of their business. Common threats included malware, ransomware, phishing and business email compromise, including invoice scams.[1]

In fact, a report was made to ReportCyber every 6 minutes in 2024 and almost $84 million was self-reported in losses due to business email compromise (BEC). BEC continues to significantly impact businesses, with an average financial loss of over $55,000 for each confirmed incident.[2]

Whether a cyber crime or data loss event is caused by human error, or is the result of criminal activity, the negative impact it could have on your business's reputation and on your customers is also severe.

In our Cyber Security Toolkit, we review the types of threats your business may face and provide a range of suggestions for staying one step ahead. We also share examples of real-life case studies where our customers have had to respond to a cyber attack.



[1] business.nab.com.au/how-to-recognise-the-red-flags-of-scams-stay-vigilant-and-safeguard-your-business-against-cyber-threats/

[2] cyber.gov.au/sites/default/files/2024-11/2023-24-cyber-threat-trends-for-businesses-and-organisations.pdf

Topics covered include:

01 What's NAB doing to help businesses?

02 Understanding what's at risk

03 NAB's tips on managing cyber security

04 Where to get further help

What’s NAB doing to help businesses?

Free cyber security protection

Enjoy the benefits of CrowdStrike Falcon®. Go cyber security free for one year with NAB’s exclusive promotional code, a saving of over $450. Enjoy award-winning, AI-powered cyber security that can help protect your business against threats, including ransomware, data theft and more. To get your promo code, log in to the NAB app or Internet Banking, or speak to your banker. Visit nab.com.au/businessoffers#security

NAB Connect integrated security

Our integrated security features on NAB Connect reduce human error risks and help to protect your business from potential threats. These include optional security features, such as segregation of duties, dual administration, customisable access and viewing rights. See more at NAB connect.

Free business cyber assessment tool

We’ve partnered with Microsoft to deliver a free cyber assessment tool, to help your business determine and improve its cyber maturity. The free, tailored self-assessment takes under two hours to complete and will provide a risk-based report to assist you to identify potential gaps and mitigate your risks. Visit nab.com.au/businessoffers#security

Free cyber safety training for businesses

We offer free online cyber security training for businesses and monthly cyber security webinars. Visit nab.com.au/cybersafetytraining

Understanding what’s at risk

It’s not just your financial information that’s at risk from cyber criminals, but details about your business, your employees and your customers. Taking stock of the information you hold, where it’s stored and who can access it is an important part of protecting your operations and maintaining trust.

More than money

Losing business data could mean losing your customers, your income and your employees. It could also damage your reputation as a trusted business. While it may be possible to recover or rebuild your business data over time, your business may not be able to operate for long, or at all, without it.

Potential data loss

Customer/Client	Business	Employees
Personal and business details	Business strategies and market intelligence	Employment contracts
Payment details and order history	Contracts and legal documents	Payroll and employee data
Name, phone number and address	Financials and accounts	Employee health/disability records
Relationship history with your business	Intellectual property	
	Product inventories	

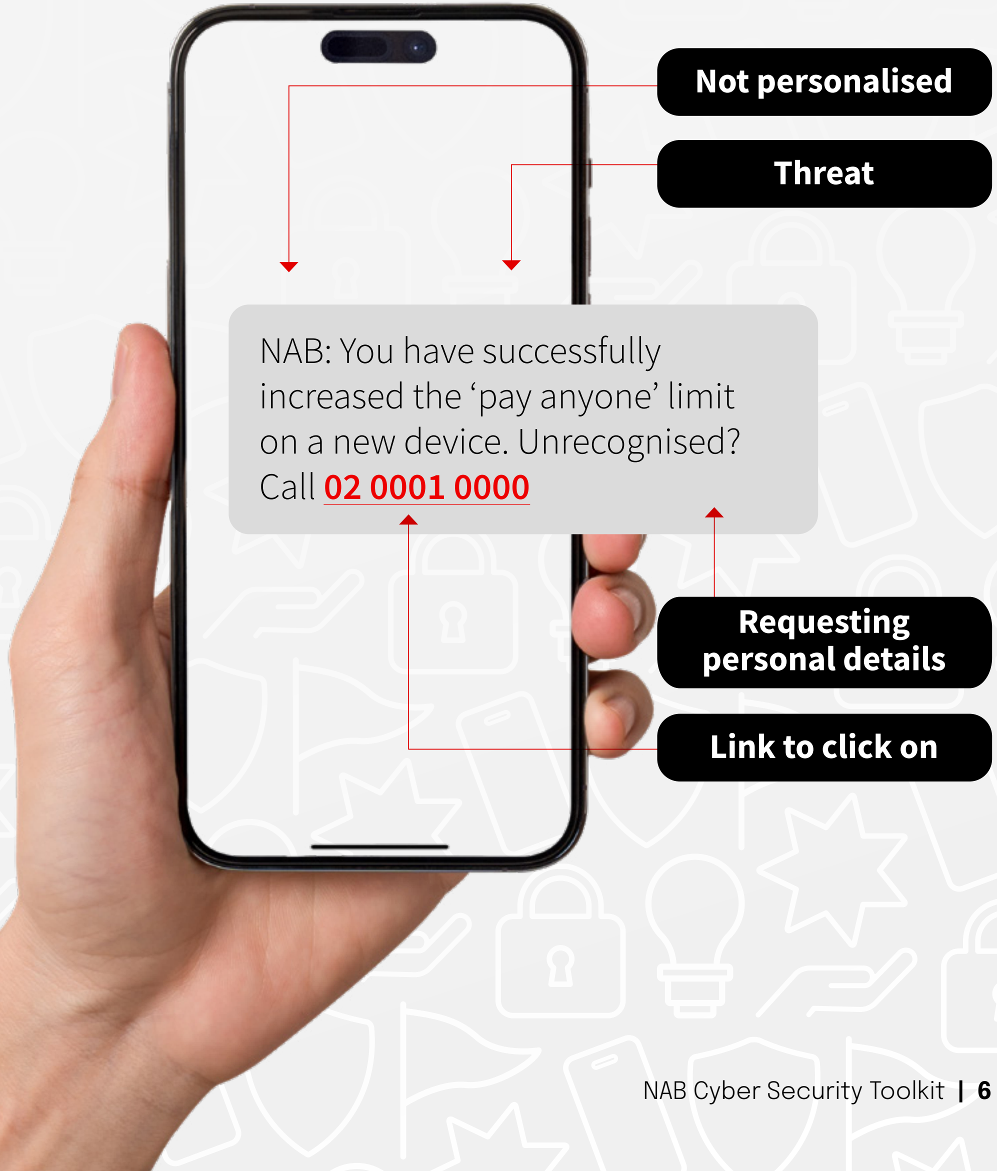
Spot the red flags

We're all doing more online than ever before. That's why it's vital you recognise the red flags and know how to protect yourself and your business.

Phishing

Criminals will do their best to make fraudulent emails and text messages look legitimate. Commonly known as phishing, the emails or messages are designed to trick you into calling an unofficial number, clicking on a malicious link, providing login personal/banking information or downloading malware. Our mobile example to the right includes signs that may help you recognise a suspicious message.

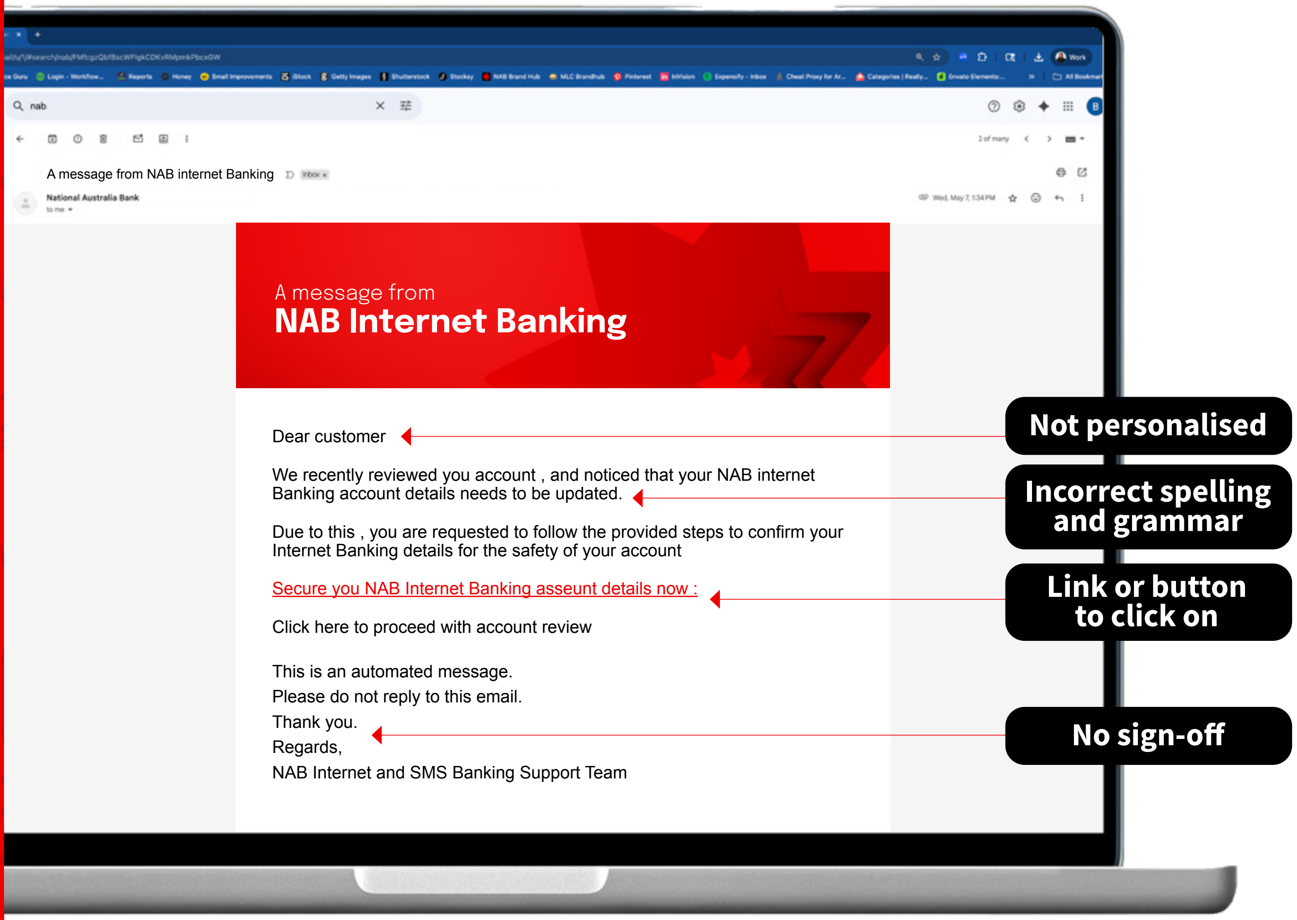
If you receive a suspicious email or text message, do not click on the links or attachments or call unofficial numbers. To visit NAB's website, always type nab.com.au into your internet browser, or use the NAB app. Not sure if a message is legitimate? Contact the organisation directly to check.



NAB: You have successfully increased the 'pay anyone' limit on a new device. Unrecognised? Call 02 0001 0000

Spotting a phishing email – an example

To the right is another example involving a real email which was sent to customers deliberately trying to impersonate NAB. It clearly shows some of the signs that the email is fraudulent, plus some of the ways the scammers are trying to defraud the customer.



A message from NAB internet Banking

National Australia Bank

A message from
NAB Internet Banking

Dear customer

We recently reviewed you account , and noticed that your NAB internet Banking account details needs to be updated.

Due to this , you are requested to follow the provided steps to confirm your Internet Banking details for the safety of your account

Secure you NAB Internet Banking asseunt details now :

Click here to proceed with account review

This is an automated message.
Please do not reply to this email.
Thank you.
Regards,
NAB Internet and SMS Banking Support Team

Not personalised

Incorrect spelling and grammar

Link or button to click on

No sign-off

Types of cyber threats

Phone and remote access scams

Criminals may call you, impersonating a bank, telco or computer company, and tell you there's an issue with your computer, banking or phone. They'll ask you to download a program that gives them remote access to your computer, so they can 'fix' the issue. However, if you do this, they can access all the information on your computer.

You should never give an unsolicited caller access to your computer. These scam calls aim to pressure you into providing your personal or banking information.

Investment scams

Investment scams promise investments with quick, high returns and minimal risks. They often involve shares, foreign currency trading, treasury bonds, term deposits, cryptocurrencies and real-estate schemes.

Whether you're looking to invest your wealth or buy a new business, knowing how to identify a scam can help safeguard your money and future goals.

Case Study:

How a trusted connection led to an investment scam

It all started when Jesse rekindled a friendship online with an old school friend, Bailey.* Bailey often shared stories of exciting new ventures and investments, including a buzzing tech start-up.

One day, Bailey asked Jesse for a short-term, 6-month bridge investment to cover consultant fees and other upfront costs for his start-up. In return, Jesse was promised high returns and priority to invest in future projects. Jesse was convinced by Bailey's warmth and the website, client testimonial and investment prospectus he shared.

Bailey sent Jesse a link to the website while on the call. Jesse made a payment within minutes, receiving a confirmation receipt and a projected return schedule.

Bailey called Jesse a week later to say the project was thriving and Jesse had already made a 5% return. Jesse was ecstatic and agreed to invest more. Over the next few months, Jesse invested a further $23,000.

A few days after the projected return date, Bailey had stopped answering calls and emails. Jesse opened WhatsApp to find Bailey had deleted their previous chats and blocked her. That's when it hit Jesse, could it be a scam and the person on the other end of the phone might not even be the Bailey she had known from her high school days?

Jesse reported the matter to the local police station immediately. The officer checked the Money Smart investor alert list and found Bailey's company was listed as a known scam operator. Jesse was devastated she had fallen victim to an investment scam. The police advised Jesse to report the incident to her bank right away. However, they warned her that an investigation could take weeks and might not result in full or any recovery.

Over the next few months, Jesse was emotionally and mentally distressed, and the losses she faced meant her business struggled to survive. Speaking to NAB, Jesse admitted that being a scam victim had impacted how she views friendships, while also setting back her business by years. Mostly, however, she just couldn't believe she had fallen victim to a scam.

Many victims of investment scams feel this way. However, it's important to remember these criminals are highly professional and highly manipulative in their approach. They know how to build trust; for example, through old friendships or as a new romantic interest. Their job is deceiving people, and they do it well.

*Names have been changed for privacy reasons.

Types of business email compromise

Business email compromise

Business email compromise is when an organisation's email account is taken over by criminals to conduct fraudulent activities such as sending fake invoices, requesting updates to bank account details, or intercepting and altering inbound payment details.

Criminals often gain access to business email accounts by sending a phishing email impersonating a trusted organisation or contact. These emails often contain links or a request to scan QR codes for information and may download malicious software to the devices. The other common way that username and password credentials are gathered is if they're exposed through a data breach.

Invoice scams occur when a business or individual receives an emailed invoice from a supplier whose email account has been compromised by a criminal. As the invoice looks legitimate, the recipient may not question the payment details and send the payment to the account controlled by the criminal. Often the contact number on the invoice has also been altered.

Another variation of an invoice scam is when a business receives a request from a supplier to cancel a recent payment or update the bank account details held on file and is asked to make the payment to a new account.

CEO scams, also known as CEO phishing, is when an email appears to come from a senior person in a business such as a Chief Executive Officer (CEO) or Chief Financial Officer (CFO), requesting an urgent transfer of funds. By making the email appear to come from a senior person, the criminals hope the recipient will action it quickly without verifying the request.

These emails may come from the real executive's email account if it's been compromised, or from a very similar email address.

Payroll scams are another type of email scam, where the email account of an employee is imitated or compromised, and an email is sent to their employer requesting an update to their bank account details for their salary.

Criminals are opportunistic and looking for people to act on messages being sent, so keep an eye out for urgent requests to update payroll details.

These scams can also be carried out via a phone call, so having a validation process for each channel is recommended.

Case Study:

How a payment request was not what it seemed

Hunter,* a property developer, received an email from his solicitor asking him to update the account details for a $650,000 settlement payment. Having worked with the solicitor before, he had no reason to doubt its legitimacy.

Hunter went to the NAB St Ives branch to act on the request. Having recently been trained to spot red flags of invoice scams, the NAB St Ives branch manager asked him questions to ensure everything was legitimate. When asked if he had confirmed the updated account details with the solicitor on the phone, Hunter mentioned he didn't think that was necessary since he had worked with the solicitor multiple times in the past.

Nevertheless, the branch manager insisted he call the solicitor on their saved or publicly listed number before making the payment. Hunter was frustrated by this request and just wanted to make the payment as soon as possible. However, the branch manager convinced him to make a quick phone call to the solicitor.

It was lucky Hunter did. The solicitor advised him that they had not changed their bank details and didn't recall sending such an email.

Hunter thanked the branch manager for saving him from a scam and decided not to continue with the payment until he had time to triple check the details with the solicitor and investigate the email further.

The following evening, Hunter emailed the branch manager advising them that he had spoken with the solicitor, who confirmed their email was compromised and a cyber criminal had sent the payment request with updated bank details to an account in their control. They also mentioned other clients had received fake payment requests as well and his call was what alerted the solicitor to investigate.

*Names have been changed for privacy reasons.

Other types of cyber threats

Malware

Malware is malicious software that infects your computer or device. Malware types include viruses, worms, trojans and spyware.

Ransomware is a type of malware that encrypts (or locks) the files on a computer, making them inaccessible. Once the malware has been downloaded onto the victim's computer, the victim will receive a ransom note to unlock the files and prevent the data from being leaked publicly.

Denial of service

Denial of service uses a network of devices to send large volumes of traffic to your network with the aim of overloading it, so it gets knocked offline and is unavailable.

What to do if your business is impacted by ransomware

The Australian Cyber Security Centre (ACSC) recommends that businesses impacted by ransomware:

- Never pay a ransom
- Disconnect devices
- Stop the ransomware
- Run a malware scan
- Write down the key details
- Get professional help
- Notify and report

You can find the full instructions on the ACSC website: cyber.gov.au/ransomware/what-to-do
You can find more information at nab.com.au/ransomware & nab.com.au/businessdisruptions

At a glance… common red flags to look out for

Suspicious emails
Criminals will do their best to make fraudulent emails and text messages look legitimate, commonly known as phishing. The emails or messages are designed to trick you into clicking on a malicious link, providing personal/banking information or downloading malware.

If you receive a suspicious email or text message, do not click on the links or attachments.

To visit NAB's website, always type nab.com.au into your internet browser, or use the NAB app.

Not sure if a message is legitimate? Contact the organisation directly to check.

Unsolicited advice
Never take investment advice from someone you've never met, especially if they contact you unexpectedly or through social media or via dating apps. Always check the investor alert list on moneysmart.gov.au for a list of companies you should avoid.

Alternative payment methods
Criminals will often ask for payments using cryptocurrency apps or ATMs.

You're asked to click on a link or scan a QR code to download an attachment or app
This is how criminals take over business email accounts, so be alert to these requests if you work for a business. It's a way for them to infect your device with a virus or direct you to a website that steals your usernames and passwords. Only download apps from official channels such as the App Store or Google Play store.

Contact details that don't seem quite right
Criminals often use fake contact details to impersonate legitimate companies and employees, so always use the contact details on a company's official website. Look out for slight differences in email addresses, such as a '1' instead of an 'i', which can be hard to spot.

You're asked for your usernames and passwords
Never share these details with anyone calling you. Remember, NAB will never ask for your login details or to log in to your banking via a link or QR code.

Requests to transfer money to a new account
If you work for a company or business, criminals may impersonate a colleague or contractor, asking for a funds transfer to be made on their behalf. Once this happens, it can be very hard to get the money back.

Remember these 3 easy steps:

STOP. CHECK. PROTECT.

If you receive a suspicious message or phone call, stop to consider, could this be a scam?

Check with the person or organisation directly to verify if the request was legitimate.

Act quickly to protect yourself if something feels wrong – hang up the phone, report the email or text, and immediately contact your bank if you've shared your banking details or notice a suspicious transaction.

STOP before you act

If an investment offer seems too good to be true, stop to consider, could this be a scam? The scam will often seem urgent and criminals will pressure you into making fast decisions, but you can take your time before you act.

If someone sends you a link, QR code or attachment – even if it looks like they're from a person or a company you trust – stop to consider, could this be a scam?

CHECK before you share

Before handing over personal information and money, check with the company directly using their official, publicly listed contact details. Also check with the Australian Securities and Investment Commission (ASIC) to see if the person providing advice has an Australian Financial Services Licence (AFSL) or Australian Credit Licence (ACL) and their investment prospectus is registered.

If you receive an email from a business with new bank account details, an invoice with updated payment instructions, or you're making a large payment to someone new for the first time, check the details are correct. You can do this by calling the company on their publicly listed number or a number you already have. Don't rely on the contact details on the invoice or email, as they may have been altered by criminals.

PROTECT if you suspect

Acting quickly if something doesn't feel right goes a long way in helping to protect your money and information, so if you think you've been scammed or your banking details have been compromised, call us on 13 10 12 and ask for our Fraud team.

Simple steps to protect your business

Empower your team

Your employees are the first line of defence against cyber attacks. Teach them to recognise and know what to do with suspicious emails, text messages and phone calls. Criminals try to convey authority by impersonating someone senior in your business or create panic by insisting a matter is urgent.

Empower your employees to trust their instincts and question emails, even if they appear to have come from someone senior. If an email request doesn't sound right, is unexpected, presses for urgent action or has an unusual tone, staff should be encouraged to question it. No one knows their colleagues, clients and suppliers better than your team. You can always invite your team to join one of our free monthly cyber security webinars for business via nab.com.au/cyberandfraudsessions

Avoid simple passwords

Use a unique, complex password for each account and keep them to yourself. Consider using passphrases, which are a combination of multiple random words containing upper and lower case letters, numbers and special characters. These are much harder for others to guess. You can even save them in a password manager tool, so you don't have to remember them.

Most importantly, disable the option on your web browser to automatically remember usernames and passwords. Never select this option as it is vulnerable to compromise. You can check your browser's help menu for instructions.

You can find more information at nab.com.au/passwordsecurity

Change your cyber culture

Help your people understand more about the tricks and scams of fraudsters. If your business gets a CEO phishing email or fake invoice, share it around so your employees know what to look out for in the future.

Build an online hub for your business's cyber safety guidelines and tips. In the interim, have them visit nab.com.au/security and nab.com.au/securityalerts, which are full of pragmatic and relevant articles, videos and training modules.

Make reporting easy. Employees need to know where to go to report cyber security threats or incidents. This could be an online form, a specific email address that is monitored regularly, speaking to a specific individual, or calling a dedicated telephone number.

Ensure learning is compulsory. If possible, offer an engaging training and assessment session or module that employees must complete within their first few weeks and then at least annually. You can find useful training videos and modules on NAB's Security Hub.

Use multi-factor authentication (MFA) or 2FA

Multi-factor authentication (MFA), sometimes known as ‘two-factor authentication’ or ‘2FA’, provides an extra layer of security for online accounts such as banking and email. When using MFA, in addition to your password, a second piece of information is required to access your account, such as an SMS code or a security token. MFA is particularly important if you have employees accessing your systems remotely.

How do I set up multi-factor authentication?

- You can set up MFA for Office 365 in the Admin Centre. This will generate a phone call, text message or an app notification to your mobile once you have entered your password. Find out more here: support.office.com
- For Apple iOS or macOS devices you can enable this function by going to your Settings > Passwords and Security section. Find out more here: support.apple.com/en-au

You can find more information at nab.com.au/mfa

Create safe payment processes

Create a process that requires the receiver to check the requester’s email address carefully, and to call them via a known or publicly listed number to confirm the request.

Check your email settings

Check your email account settings for any auto-forward rules that you didn’t set up yourself, as this can be a sign that emails are being forwarded to another account. Also check the ‘Sent’ and ‘Deleted’ folders periodically for emails you did not send. If they are empty, this can be a sign that evidence is being deleted.

Update your defences

Always keep your operating system and applications up to date

Always upgrade your operating system when new versions become available, as they often include enhanced security features and bug fixes. Make it easy for yourself by setting up automatic updates and installation to keep your devices protected and up to date with the latest operating system vulnerabilities.

Install a firewall to block unwelcome access

A firewall is a protective security system that monitors and manages traffic between your computer network and the internet. It filters traffic types that can reach your network based on a set of defined security rules. If incoming traffic breaches a security rule, that traffic will be blocked from reaching your network.

Keep your anti-virus and malware protection up to date

Anti-virus software is a tool to protect your computer or network from cyber security threats. If a threat is detected, you receive an alert, along with the recommended action you need to take. Check if your operating system offers inbuilt anti-virus and malware protection. If not, speak to your trusted IT retailer. The key to staying protected is to set up automatic updates for your anti-virus software.

Protect your data with encryption

Encryption software protects your data by disguising it in a code that unauthorised people can't view, even if they have physical access to it. Search the support pages of Microsoft or Apple security to find out how to turn on encryption for data security.

Back up your data regularly

If your system is compromised, you're at risk of losing all your business data. Make sure you back up your data regularly. Also test your back-up regularly to ensure it contains what you need to run your business if your systems are compromised.

Be vigilant on access management

Employees in your business should have their own login credentials to business systems. Remove administration rights from computers that don't need it. Don't browse the internet using an administration account. This prevents the entire network from becoming infected if a compromised website is visited. Ask your IT provider if they have remote access to your systems and what security controls they have in place. Ask your IT provider if they use different passwords for each of their customers' sites.

Secure your mobile phone

Your mobile phone or tablet is the portal to almost every detail about you so it's important to keep it secure. Lock your phone either with a password, PIN, fingerprint or face ID. Update your phone's software to keep up to date with security settings and bug fixes. Back up irreplaceable data, such as photos or emails, through reputable and secure 'cloud' storage solutions. Turn off Bluetooth when you're not using it. Download apps from trusted online stores such as Google Play or the App Store. Log out of websites, such as your online banking account, when you've finished using them.

What to do if you experience a cyber event

If you believe your business has been affected by fraud, scam or cyber crime, it's important to act quickly.

Seek assistance from your IT provider or internal security team right away.

The Australian Cyber Security Centre (ACSC)

Report a cyber crime, scam or fraud: cyber.gov.au/report

The Office of the Australian Information Commissioner (OAIC)

Seek assistance from the OAIC at oaic.gov.au for a reportable data breach.

An eligible data breach is an unauthorised access to or disclosure of personal information; serious harm to the individuals to whom the information relates; the organisation has been unable to prevent the likely risk of harm with remedial action.

Your financial institution

If you have provided your banking credentials or notice a fraudulent transaction on your account, contact your bank immediately.

NAB's number can be found on the back of your card. You can also report suspicious NAB-branded emails and SMS to phish@nab.com.au or text 0476 220 003.

The ASD Essential Eight

You also need to secure your computers, networks and systems. While no set of mitigation strategies can entirely protect you, it's recommended you follow the eight essential mitigation strategies by the Australian Signals Directorate. These practical actions aim to help prevent malware from running, limit the extent of an incident, as well as help recover your lost data.

See cyber.gov.au/essential-eight

Stay up to date

Criminals change tactics all the time, so it's important to stay up to date with the latest information.

To do this, visit:

NAB Security Hub: nab.com.au/security

The Federal Government's Australian Cyber Security Centre: cyber.gov.au

The Federal Government's Scamwatch service: scamwatch.gov.au

Australian Government eSafety Commissioner: esafety.gov.au

Australian Competition and Consumer Commission (ACCC): accc.gov.au

NAB Secure

The information in this document is provided for general information purposes only. National Australia Bank Limited (ABN 12 004 044 937) or its licensors do not warrant or represent that by following the steps in this document you will not be subject to an adverse cyber security incident. NAB does not warrant or represent that the information in this document is complete or free from errors or omissions or is suitable for your intended use. Before acting on any information in this document, NAB recommends that you consider whether the information is appropriate for your circumstances. Subject to any terms implied by law and which cannot be excluded, NAB accepts no responsibility for any loss, damage, cost or expense (whether direct or indirect) incurred by you as a result of any error, omission or misrepresentation in any information in this document. Links to third-party websites are provided for your convenience. These third parties are not affiliated with NAB, and NAB is not responsible for and does not control the content of their sites. Links to third-party websites are provided for yourconvenience. These third parties are not affiliated with NAB, and NAB is not responsible for and does not control the content of their sites. By clicking on these links, you will exit NAB's website and be taken to the third party's website. Any personal information you provide to the third party's hosted site will be collected, used, disclosed, and secured in accordance with their Privacy Statement, Privacy Policy, and security practices.

© 2025 National Australia Bank Limited ABN 12 004 044 937 AFSL and Australian Credit Licence 230686. A182041-0825