

more
than
money



Your business and cyber security

Learn how to protect your business
from cyber threats



NAB's tips on managing cyber security for small business

Malicious cyber activity is increasing in frequency, scale and sophistication according to the 2020 Australian Cyber Security Centre (ACSC) annual cyber threat report.

The NAB Cyber Security Survey of 2020 found that 6 in 10 Australian businesses have been victims of a cyber security incident in the last year, and fewer than 2 in 10 are very confident that they have

the right controls in place. Cybercrime costs the Australian economy \$33 billion annually, as well as impacting businesses' operations, reputation, emotional and psychological wellbeing. Cybercrime has also resulted in the closure of a growing number of small businesses.

What does a cyber threat or attack look like?

Here are some common examples:



Phishing messages Emails or text messages attempting to trick you into clicking on a malicious link, providing login credentials, personal or financial information to an unauthorised source.



Denial of service Using 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.



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



Business Email Compromise 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.



Ransomware Locking or encrypting the files on your device so they're unusable, and then demanding a ransom payment to return this information back to you.

Understanding the value of your data

Protecting your business data is as important as protecting your physical assets. While insurance can cover the cost of replacing building infrastructure, inventory, machinery and equipment or vehicles, business data is not so easily replaced.



What data does my business have?

Think about all the databases and information you've invested time and effort in building over the years, including your customers':

- Personal and business details
- Payment details and order history
- Name, phone number and address
- Relationship history with your business.

As well as business records such as your:

- Business strategies and market intelligence
- Contracts and legal documents
- Emails and attachments
- Financials
- Intellectual property
- Marketing database
- Payroll and employee data
- Product inventories
- Taxation records – past and present.

Your business data can be an attractive target for criminals

Criminals attempt to gain access to data via phishing, malicious software or network vulnerabilities. This is called a data breach. The stolen information might then be used for criminal purposes such as targeting customers with spear-phishing emails, stealing their identities, or compromising your bank accounts or payment processes. They might also sell data to other criminals or to your competitors.

Computer systems may be targeted with ransomware, which encrypts your files, rendering them useless and then asking for a sum of money to decrypt the files.

In addition to the malicious threats posed by cybercriminals, consider the damage that can be caused by your own employees, such as:

- Accidentally sending confidential information to the wrong person
- Losing a phone or storage device with customer information on it

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



How much would it cost to recover lost data?

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.

Know what you have

Knowing what you have is the first step towards a strong risk-based approach to security. Identify all connected devices such as desktop computers, laptops, smartphones, printers and applications including email, software, web browsers and websites so that you can take steps to secure them.

Many cyber security incidents can be prevented by applying basic computer security practices, controls and software programs.

Once you have an inventory of all your devices and applications, you can start by taking these simple steps:

- **Keep your business computer for business use only.** Using your business computer for social media, playing games, watching videos or downloading music increases the chances of exposure to malicious software.
- **Uninstall programs that are not used.** Get familiar with the programs you use and expect to see so that any unwelcome or malicious programs will stand out. If you're not using it, get rid of it.

- **Know who is using what and why.** Your employees should have their own login credentials to business systems. Remove administration rights from computers that don't need it. Make sure your IT provider has solid security controls, including different passwords for each of their customers' sites.
- **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 and blocks traffic types that can reach your network based on a set of defined security rules. Search the support pages of Microsoft and Apple iOS for information about firewalls for your operating system.



Update your defences

Now you know what devices you have, what applications and programs you use, and who in your business is using what and why, you can now take steps to make your IT as secure as possible.

Take action to update your cyber defences by:

- **Always keeping your operating system and applications up to date.**
The most common types of operating system are Microsoft's Windows platform or Apple's Mac OS X. 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.
- **Always keeping 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.



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.

You use your phone to carry out daily tasks from wherever you are, including storing passwords to access all the information you store about yourself online. In the wrong hands your phone gives cyber criminals access to your online banking passwords, credit card details, personal and work connections, photos and videos and everything that identifies you, as you.

Always:

- 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.
- Backup 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 iTunes Store.
- Log out of websites, such as your online banking account, when you've finished using them.

You can find more information here:

nab.com.au/businessdata

nab.com.au/datastorage

nab.com.au/businessdisruptions



Beyond simple passwords

You wouldn't just give anyone a key to your business premises. And you certainly wouldn't use the same key for your home and your car. But that is exactly what using the same password for every device and account is like. Ensure you use a unique, complex password for each account and don't share them with anyone.



Security Tip

How to create a strong password

Strong passwords have a minimum of 10 characters and use a mix of:

- Uppercase and lowercase letters
- Numbers
- Special characters like !, &, and *.

Avoid using personal information such as your children, partner or pet's name, favourite football team or date of birth as your password, as they can be easy for others to guess. Also avoid using these common password combinations that criminals often look for:

- A keyboard pattern like qwerty
- Repeated characters like zzzz
- Personal information like your date of birth or driver's licence number.

How can I remember them all?

There are programs and apps known as 'Password Safes' that will store all your passwords in a secure vault. A Password Safe only needs one strong password or passphrase to access it and has extremely strong protection to make sure that only you can access it. This means you only need to remember one password or passphrase, and the safe creates and remembers the rest. Password Safes can even generate new, complex passwords for you when you create new online accounts.

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

You can find more information here:
nab.com.au/passwordsecurity



Security Tip

Set up multi-factor authentication

Multi-Factor Authentication (MFA) is a method of confirming your identity in order to access an account, which requires extra information in addition to a username and password. You will only be able to access an account after providing two or more pieces of

evidence proving your identity. This makes your accounts much harder to break into than if you were only using a password. Even if a criminal does obtain your password, they will still have to get past at least one other barrier to access your account.

MFA is particularly important if you have employees accessing your systems remotely.



Security Tip

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

- Websites such as Twitter and Paypal have options for MFA. Check if your other online accounts offer MFA here: twofactorauth.org
- 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 here nab.com.au/mfa

Avoid the lure of phishing messages

What is phishing?

Phishing (pronounced ‘fishing’) emails or text messages are designed to trick you into providing personal information like your mobile number, usernames and passwords or your credit card or bank details. Phishing messages often pretend to be from legitimate companies such as banks, courier companies, or government departments, and can contain links to fake websites. These fake sites can look very similar to the real ones, including NAB’s, and are designed to trick people into entering their bank details. NAB’s Security team monitor the internet for fake NAB websites and request to have them removed from the Internet to protect NAB’s customers.

Sometimes phishing emails will have an attachment that appears to be an invoice or document. When you try to open the attachment, it installs malware on to your computer without your knowledge. NAB has a dedicated Security Hub found at nab.com.au/security where security alerts are regularly published. These alerts include examples of the most recent NAB branded phishing attempts.

Examples


You are in control with phishing. Phishing messages are usually sent to large groups of random recipients at one time. You can outsmart criminals by taking a few seconds to check for red flags, including:

- Unusual, misspelled or slightly different email address
- Asks for personal details
- Generic greetings and sign offs
- Creating a sense of urgency or reward
- Contains links to click or attachments to open

Where possible, access your online accounts by logging into the organisation’s official app or visiting their website directly. Don’t access online services by clicking on links in messages.

Example phishing messages

From: [NAB Support](#)
Sent: Wednesday, 28 October 2020 10:53 AM
To:
Subject: [IMPORTANT] NAB#7482267 your account has been limited for security reasons.



NAB#7482267

We noticed some unusual activity on your account and are concerned about potential unauthorized access. We need your help resolving this issue, and for your safety, we have temporarily limited what you can do with your account until you take action.

What do I need to do?

[Log in](#) to your NAB account and complete the steps required to re-secure your account.

NAB - Your Internet Banking services have been suspended pending device verification. Visit <https://nab.com.au/bankingsecurity.info/> to perform verification.

You can find more information here:

nab.com.au/phishing

And see examples here:

nab.com.au/securityalerts

Phone Calls

Criminals may call you, impersonating a government agency such as the Tax Office, an energy or telecommunications provider, Australia Post, a bank or the police.

The aim of these scam calls is to pressure you into providing your personal or banking information. The caller may threaten you with expensive fines or tax bills, arrest or deportation, to take you to court, or to disconnect your internet service.

They may ask you to buy gift cards, iTunes vouchers, Crypto currency or pre-paid credit cards to pay your fine or debt. In other cases, they may request remote access to your computer and/or bank accounts to investigate an 'issue' or stop a transfer.

Legitimate businesses will never threaten to arrest you or demand immediate payment of a tax debt or fine with unusual payment methods like gift cards or crypto currency, or request remote access to your computer.



Security Tip

Tips to stay safe

- Treat any unsolicited phone calls with caution. If you're unsure about the legitimacy of any call, hang up, and call back on an official phone number to verify the call was legitimate.

- Never provide personal or banking information on unsolicited calls, via email or text message.
- Never give an unsolicited caller or unknown person who contacts you via email or text remote access to your computer or online bank accounts.

You can find more information here:

nab.com.au/phonescams

Defend against viruses and ransomware

Malicious software or 'malware' describes viruses, worms, trojans, spyware, ransomware and other malicious programs. It is commonly spread using convincing emails such as traffic infringement notices, parcel collection notices and electricity bills.

The goal of cyber criminals is to stop your computer from working properly, disrupt your business or gain unauthorised access to your personal information for financial gain.

Frequently criminals use a type of malware called 'ransomware'. It works by encrypting or locking all your files, documents, photos, videos and music-making them inaccessible. It then presents a pop-up window demanding a ransom be paid in order to regain access to the files. Unfortunately, without the encryption key, it is impossible to regain access to your locked files. For a small business this can lead to business disruption, reputational and financial impacts.



What to do if your business is



Security Tip

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](https://www.cyber.gov.au/ransomware/what-to-do)

You can find more information here:

nab.com.au/ransomware

nab.com.au/businessdisruptions



Business email compromise and invoice scams

The threat of email scams for businesses is very real, and it's growing. Based on a report from the ACCC, the most financially damaging business email compromise scams involved invoices between businesses, suppliers or individuals being intercepted, and amended with fraudulent banking details.

Business email compromise scams accounted for the highest losses in 2019, with the Australian business community, and some individuals losing \$132 million in total.

Business Email Compromise (BEC)

Business email compromise describes when an organisation or individual'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 which appears to come from a trusted organisation or contact. This email might request the recipient's email account username and password, or ask them to click on a link which downloads malicious software onto their device. Often the phishing email has been sent from a trusted contact who has had their own email account compromised. The other common way that username and password credentials are gathered is if they are exposed through a data breach.

Invoice scams

In invoice scams, a business or individual receives an emailed invoice from a supplier whose email account has been compromised by a criminal. The criminal has been able to alter the payment details on the invoice to an account they control. 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', a CEO scam is when an email is sent which 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 are hoping 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.



Security Tips

Raise awareness

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.

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 using the contact details you have on file.

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.

Keep your software up-to-date

Cyber criminals always try new ways to outsmart anti-virus software. It's vital you have the most up-to-date version. Set your anti-virus software to auto-update, so it is always up to date. Keep your Apps on your computers and devices up to date too.

Use strong passwords and multi-factor authentication

Using strong passwords and multi-factor authentication (MFA) will protect the security of your email account. Two-factor authentication means adding an extra layer of security by using an extra authentication method, such as a code sent to your mobile phone via SMS. This means that even if someone steals or guesses your password, they will not be able to get into your account because they will not have the MFA code.

You can find more information here:
nab.com.au/emailscaams

Protect your brand

Just like locking your doors each night, make managing cyber security a day to day priority and practice. Take the time to educate yourself and your employees about the ways your business could be attacked and the steps you can take to protect yourselves and the business.

All hands on deck

It starts at the top. Cyber security is not just the responsibility of your IT provider. In fact, the person responsible should be in management and have access to your data and assets.

But remember, cyber security is everyone's responsibility. You must make cyber security a part of the culture of your business. Talk openly with your employees about how they can play a role and be the first line of defence.



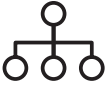


Security Tip

Change your cyber culture

You don't need a big budget to create a cyber safe culture. Here are some ideas for raising awareness about cyber safety with employees:

- Provide helpful information and tips and share examples. Build an online hub for your business' cyber safety guidelines and tips. In the interim, have them visit NAB's Security Hub and Fraud Alerts pages 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.
- Make learning compulsory. If possible, offer an engaging learning and assessment training session or module that employees must complete in the first few weeks of starting and then at least annually. You can find useful training videos and modules on NAB's Security Hub.
- Make flexible working secure and easy. Put the right secure flexible working tools and guidelines in place.



It starts at the top

It starts and finishes with people in management.

Put at least one person in your business in charge of cyber security. Someone in management with access to your data and assets.



Get everyone on board

You need to have support from everyone in the business.

From top to bottom. Just like locking your doors each night, make cyber security a day to day priority.



It's a hands-on effect

There is no single fix for cyber security. You can't solely rely on anti-virus software to keep you safe from attacks.

Educate yourself, staff and customers. Encourage staff and customers to report incidents and anything that seems out of place.



Know your risks and vulnerabilities

If you use the internet, you are at risk. Understand the ways your business can be attacked.

Perform regular checks and audits of your online "footprint" so you can prioritise your risks.



Protect your business

The right approach for you depends on your business, the people in it and the information you need to protect.

Secure your Point of Sale systems, mobile devices, networks and stored data and learn advanced techniques to become cyber secure.

Daily practices to protect your business

1. Be wary of unexpected, threatening or poorly written emails. Train your employees on how to spot and report suspicious emails and text messages.
2. Make sure your operating system and anti-virus software are always up to date.
3. Back up your data.
4. Create an incident management plan.

The recommended place to go for a comprehensive list of practical actions to make your computers, networks and systems more secure is the Australian Signals Directorate's (ASD) Essential Eight which aim to prevent malware from running, and to limit the extent of the incident and recover your lost data.



What to do if you have a cyber event?

If you find that a cyber event has occurred in your business seek assistance from:

- The Australian Cyber Security Centre (ACSC) who manage the 'Report Cyber' function: cyber.gov.au/acsc/report
- The Office of Australian Information Commissioner (OAIC) if it is a reportable data breach: oaic.gov.au
- Your financial institution if you have provided banking credentials or authorised a fraudulent payment.

Useful security resources for your business

[NAB Security Hub](#)

[Australian Cyber Security Centre](#)

[Report Cyber](#)

[Australian Government Essential Eight](#)

[Australian Government eSafety
Commissioner](#)

[Australian Competition and Consumer
Commission \(ACCC\) Scamwatch](#)

© National Australia Bank Limited (ABN 12 004 044 937) or its licensors. The information in this document is provided for general information purposes only. NAB does 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 in this document 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.

© 2022 National Australia Bank Limited ABN 12 004 044 937 AFSL and Australian Credit Licence 230686 A160078-0422