Helping you and your business be safer online

bnz

Cyber security can be a big problem for small business

Businesses are twice as likely as individuals to fall victim to scams, according to research conducted by BNZ and Camorra.*

To help New Zealanders and their businesses be safer online, we've developed a suite of resources to help you take practical steps to enhance your online security and protect your business from cybercrime.

So what exactly is a cyber threat or attack?

Phishing messages

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

Malware

Malicious software that infects your computer or device. Malware types include viruses, worms, trojans, spyware, and adware. Malware is typically delivered via attachments in emails.

Ransomware

Locking or encrypting files on your device so they're unusable, and demanding a ransom payment to return them. This could also involve theft of information. Ransomware is typically delivered via attachments in emails.

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 becomes unavailable.

Data loss

Where information is stolen from a system or an accidental privacy breach from emailing information without due care.

*BNZ research conducted with Camorra Research Ltd in July 2023 - SME research, sample size of n=602 (business)

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, equipment, or vehicles, business data is not so easily replaced.

What data does my business have?

Data is the lifeblood of your business. You might not realise it, but the success of your business depends on it.

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 worth a lot of money in the wrong hands

Criminals can infiltrate your computer systems, via phishing or malicious software, in order to steal your business data and sell it to other criminals or your competitors.

Or your computer systems may be targeted with ransomware, which encrypts your files, rendering them useless.

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

- accidently sending confidential information to the wrong person
- losing a phone or storage device with customer information on it.

Whether by human error or crime, the result for your information, your business, and your reputation is the same.

Know what you have

Knowing what you have is the first step to better security. Identify all connected devices such as desktops, 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 programmes.

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

- **Conduct a risk assessment.** Understand your critical information, processes, systems, and privileged access users key to your business operation. Knowing the risks your business faces can help you prevent or efficiently recover from an incident. Bring in expertise to help you quantify the risks, threats, and preventative controls specific to your business.
- **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 programmes you use and expect to see, so any unwelcome or malicious programmes 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.

Update your defences

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

You can take action to update your cyber defences in the following ways.

- **Always keep 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.
- **Always 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.

- **Update your default passwords.** Systems and software are provided with default login details that give the user administrator-level access to a product. They should only be used for the initial setup, and then changed afterwards. Default passwords are easy to guess or find online. Attackers could use them to get into your system.
- **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.
- **Enforce the principle of least privilege.** The principle of least privilege means granting users the minimum level of access they need to perform their job. This prevents users from either accidentally or intentionally making changes that can cause security incidents. It also prevents an attacker from getting very far into the system or network if they manage to steal a user's password.

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.

To keep your mobile phone secure you should always do the following.

- 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.
- Download apps from trusted online stores such as Google Play or the Apple App Store.
- Log out of websites, such as your online banking account, and your email account when you've finished using them. A scammer could use the forgotten password feature of another service, and receive an email with a link reset and login.

Passwords and multi-factor authentication

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 application is like. It's a good idea to have different passwords for every site or device - and never share your passwords amongst business colleagues or family.

Multi-Factor Authentication (MFA) is the most common term for the method of confirming your identity in order to access an account, which requires extra information in addition to a username and password. It is sometimes referred to as two-factor or two-step authentication. You will only be able to access an account after providing two or more pieces of evidence proving your identity.

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 or email remotely, where a scammer could use the forgotten password feature of another service, and receive an email with a link reset and log in.

Security tip

How to create a strong password

- One of the best ways to protect confidential information, and help keep your business safer online, is with strong passwords.
- Make your password long and strong: sentences or passphrases are best because they are easier to remember. In fact, a passphrase of four or more words are collectively stronger than a 10-character password using a mix of characters, symbols and numbers, and easier to remember. For example, myletterboxiswhite.
- Use a different password for every online account: that way if a scammer gets hold of one of your passwords, they can't access your other accounts.
- Keep your passwords safe: using a password manager (protected by a strong password or passphrase) means you only need to remember one set of login details to access all your passwords.
- Don't use personal information: it's easy for scammers to find online. Likewise, don't use information available online to create a password.

How do I set up a multi-factor authentication?

- You can set up MFA with your email provider. This will generate a phone call, text message, or an app notification to your mobile once you have entered your password.
- Social media websites have options for MFA. Check if your other online accounts offer MFA at www.cert.govt.nz/individuals/guides/two-factor-authentication

Security tip

How can I remember all my passwords?

There are programs and apps known as password managers that will store all your passwords in a secure vault. A password manager 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 managers even generate new, long passwords for you when you create new online accounts. Browsers like Microsoft Edge or Chrome have inbuilt password managers. A message will pop up asking if you want the browser to save your password for you when you log in to a site. While this might seem like a good option, it's not as secure as using a dedicated password manager and is not recommended if you share a computer with another person.

Browsers will usually store your passwords on your computer. This means that if you leave your computer unattended or unlocked, other people could get easy access to your password details. You can check your browser's help menu for instructions.

Don’t get caught in a criminal’s net

What is phishing?

Phishing is a cybercrime in which a target is contacted by email, or text message by someone posing as a legitimate institution to lure you into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

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 look very similar to the real ones, including BNZ’s, and are designed to trick people into entering their bank details.

BNZ’s Cyber Defence team monitor the internet for fake BNZ websites and will report them to the appropriate authorities to protect BNZ’s customers. You can help by forwarding any suspicious phishing emails to **phishing@bnz.co.nz**

Sometimes the 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.

BNZ has a dedicated space where security alerts are regularly published.

Visit **bnz.co.nz/latestscams**

Security tip

Tips to stay safer from phishing

BNZ will never text a web link. If you receive one, this is a scam

- Scammers hide fake sites behind normal looking links. Hover over links to see what website the link is actually taking you to. Advanced tip - tap and hold on a text message.
- Some of the more sophisticated phishing attacks can come from a legitimate account of someone you know. If you receive an unusual link or attachment you were not expecting, follow up with a phone call to ensure it is legitimate before opening.
- Always manually enter any financial sites using your web browser. Never login to your bank via a link sent to you.
- Criminals can use phishing emails to capture credentials to email accounts to pose as someone you know. Make sure you use multi-factor authentication to protect against this attack, and if you receive any suspicious emails such as those asking to change bank account details for invoice payment, always follow up with a phone call to ensure the legitimacy of these requests.
- Verify payments using the phone number provided on the sender's official website. If you receive an invoice with an updated bank account, call them directly to confirm. Don't use the contact details on the invoice or in the email, these have likely been changed by the scammer.

Emails

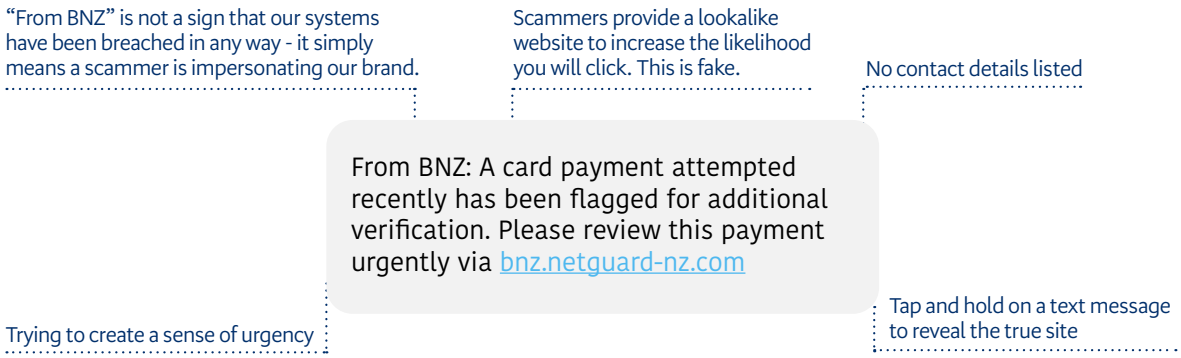
The phishing email you may have received was probably sent to several thousand other people as well. You have the opportunity to outsmart these criminals by taking a few seconds to look for the signs of a scam, including:

- a sense of urgency
- the sender's email address looking unusual, misspelled, or slightly different
- generic greetings and sign offs
- poor grammar and spelling
- suspicious links and fake websites.

Do not reply, or open links or attachments from suspicious emails.

Text messages

Like emails, stay in control by not replying to or opening links in suspicious messages. Here is an example of a phishing text:



BNZ will never text you with a link.

Phone calls

Criminals may call you impersonating a government agency such as Inland Revenue, an energy or telecommunications provider, New Zealand Post, a bank, or the New Zealand Transport Agency.

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 disconnect your internet service.

They may ask you to buy gift cards, iTunes vouchers, cryptocurrency, or pre-paid credit cards to pay for this fine or debt. Scammers may attempt to access your computer by requesting you download remote access software such as TeamViewer or AnyDesk. Never do this! Hang up and contact the company the scammer said they were representing on a number you already know or on their website.

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

Security tip

Tips to stay safer

- 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 if the call was legitimate.
- Never provide personal or banking information on unsolicited calls, or 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.

Defend against viruses and ransomware

Malicious software or ‘malware’ describes viruses, worms, trojans, spyware, ransomware, and other malicious programs. It’s 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.

More and more frequently these criminals are using a type of malware called ‘ransomware’. It works by locking all of your files — documents, photos, videos, and music — and 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’s impossible to regain access to your locked files. For a small business this experience can be at best expensive and disruptive, and at worst can result in the company going out of business.

A key step to staying protected is to set up automatic updates for your anti-virus, malware and threat protection software.

Security tip

How Cert NZ critical controls can help you stop a ransomware attack in its tracks.

www.cert.govt.nz/assets/ransomware/cert-lifecycle-of-a-ransomware-incident-with-controls.pdf

- Isolate the infected computer from the network to prevent the software spreading.
- Restore your system from your most recent backup.
- Reinstall your operating system if you don't have a backup – but note that this may erase all of your files.
- Talk to your IT support person or a local computer services company if you need help with anything. They can:
  - check to see if you have 'real' ransomware on your computer — attackers sometimes install fake ransomware to scare people into paying them
  - try to get rid of ransomware from your computer — depending on the type of ransomware it is
  - restore your computer to its factory settings and rebuild it for you if they can't get rid of the ransomware — this may also erase all of your files
  - advise you on security to protect yourself in the future
  - install security protection for you.
- NZ Government advice is to not pay the ransom. It will not guarantee your files will be returned and it can make you a target for further attacks. www.dpmc.govt.nz/our-programmes/national-security/cyber-security-strategy/cyber-ransom-advice

Protect your brand

Just like locking your doors each night, make cyber security a daily priority and practice.

Take the time to educate yourself, your employees, and your customers about the ways your business could be attacked and the simple 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 or employees. 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. Emailing a list of rules to staff won't cut it. Don't focus on scare tactics or what your employees can't do. Talk openly about what they can do to help keep your business and customers safe.

Security tip

Change your cyber culture today

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.

- **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, a specific individual, or a telephone number. Mistakes can happen so it's important that your employees know where to go to get help.
- **Provide helpful information and tips.** Build an online hub for your business' cyber safety guidelines and tips. In the interim have them visit Get Scam Savvy / bnz.co.nz / CERT NZ.
- **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.
- **Make flexible working secure and easy.** Put the right secure flexible working tools and guidelines in place.

1. 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.

2. 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 daily priority.

3. It's a hands-on job

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.

4. Know your risks and vulnerabilities

Understand the ways your business can be attacked. Perform regular checks and audits of your online "footprint" so you can prioritise your risks.

5. Create a plan for when things go wrong

Having a clear plan in place will help you through what could be a stressful time. It'll help your team respond to an incident quickly, and improve your business' resilience.

Run through simulation exercises to test how and who would respond to each identified cyber threats, including preparing for media responses should customer data be exposed.

What to do when things go wrong

Unauthorised access to your business information via a compromised email account or cloud storage could constitute a privacy breach. If your business experiences a privacy breach, you may have to report it to the Office of the Privacy Commissioner (OPC) under the Privacy Act 2020, and inform all your customers whose information might have been affected where it is considered a notifiable privacy breach – unless certain exceptions apply.

An incident like this can damage a business' reputation and customer trust.

Remember to do the following:

- Talk openly with your employees about what they can do to keep your business and customers safe.
- Report cyber security threats and issues to Cert NZ.
- Under the Privacy Act 2020, if your organisation or business has a privacy breach that either has caused or is likely to cause anyone serious harm, you must notify the Privacy Commissioner and any affected people as soon as you are practically able.

Use this tool to help you determine whether a breach is notifiable
www.privacy.org.nz/responsibilities/privacy-breaches/notify-us/

Get Scam Savvy

When in business it is important to know the types of scams that impact New Zealand businesses. Learn how to identify scams with www.getscamsavvy.co.nz/business

13560 08.23