Financial crime is everyone's business.

How to create a culture of crime awareness in your organisation.

"As businesses work towards strengthening their IT defences, fraudsters are starting to focus more on compromising people rather than systems. All it takes is one staff member (or even the CEO) to click a link in a phishing email or miss the red flag in a payment request and your business could lose a lot of money or suffer reputational damage. Empowering your people to understand the tactics fraudsters use – as well as regularly reviewing your fraud defences – will give you the best chance of preventing financial crime."

Tracey Brown, Senior Manager Financial Crime, Westpac New Zealand.

Financial fraud and scams targeting businesses are on the rise – globally and in New Zealand.

Right now all types of data are for sale on the dark web – like usernames and passwords for email and bank accounts, stolen credit card numbers, identity documents and contact details. These can be used by fraudsters to impersonate employees, customers and suppliers. As a result, we're seeing an increase in scams like invoice, payroll payment and transactional payment fraud.

According to the Serious Fraud Office[1], these types of crimes are underreported by businesses in New Zealand because they are concerned about reputational risk if the cases are publicised, so we don't actually know the true scale of the problem. What we do know is the majority of these scams are carried out by email.

When you're thinking about how to approach fraud awareness in your business, start with the assumption that everybody in your organisation could be compromised.

It used to be fairly easy to spot a spoof email. But fraudsters have evolved their methods. Not only have they become better at faking emails and websites (and using the correct spelling and grammar), they've also become very good at using psychological tactics to get people to action requests quickly. Everyone in your organisation is at risk – whatever type of business you're in.

For instance, a staff member may get an email that looks like it's come from the CEO. The email could ask them to pay an invoice on the CEO's behalf urgently, or provide private staff details. A CEO can also be targeted. They may receive an email asking them to click on a link to confirm their login details on the company website, which has been faked to look just like the real thing. Or an email may go out to staff that looks like it's from HR, asking them to log into the HR system and change their password.

Fraudsters will take advantage of your people's desire to be efficient, or play on their fear of doing the wrong thing to get the information they want. And once they have access to your systems, they can cause untold damage by attempting to steal money, locking you out until you pay a ransom or threatening to cause reputational damage by releasing sensitive information.

As a society, in New Zealand we tend to put a lot of trust in email and electronic invoicing. This means we're often not as vigilant as we should be. Think about how you operate when you're in your inbox. Are you methodical and deliberate about checking each email? Or are you operating on autopilot – being fast and efficient, automatically replying and actioning each request in between other jobs? While the second option certainly gets the job done faster, it can make it harder to spot the types of sophisticated scams we're seeing as a bank.

How the scams work.

Payroll payment fraud.

Fraudsters have been targeting New Zealand educational institutions in particular with this scam. The fraudsters (usually operating from an overseas IP address) create a false email address in the name of an employee, then email their payroll department requesting a change of bank account. The employee's salary is then paid to the fraudsters instead of the employee.

Business invoice fraud.

This scam targets businesses of all sizes – even small, local sporting clubs and community groups. Any organisation that transfers money via bank accounts is a potential target.

The typical pattern is that the criminal gets access to the business email account, waits until an invoice is actually being sent out, then intercepts the email and edits the account number on the invoice. Everything looks legitimate, so it's not uncommon for this type of fraud to go entirely undiscovered until months later when the company whose email account has been hacked realises they haven't been paid, or customers call to find out where their goods are.

1 **Source:** nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11870607

Fraudsters attempt to clean out cleaning supply company.

When a cleaning supply company received an email from a supplier, notifying them of a change of bank account, along with a $50,000 invoice to pay, nothing seemed suspicious[2]. The email came from the supplier's correct email address, so it looked genuine. The cleaning company logged the $50K payment and didn't even know there was an issue until the Westpac NZ Fraud Team contacted them and told them the transaction had been blocked.

Westpac's fraud team had already frozen this particular fraudster's bank account and were looking into their activity due to a previous transaction that had alerted the bank. Since that fraud attempt, the business has implemented new measures. They have increased their security settings, so no one is authorised to do email forwarding. And if there is any request to change bank account details or contact details, staff now also have to physically check and verify with the supplier before changing their payment details.

The past-due invoice scam.

To date, this scam has largely targeted tradespeople and builders in New Zealand. The business receives an email that appears to be from a trusted vendor containing an urgent request to pay a past-due invoice – usually with a very realistic-looking forgery attached. The business then pays the invoice into the fraudster's bank account instead of the vendor's bank account.

Real estate scams.

Fraudsters use various methods to get their hands on house deposits or real estate settlements. One way they do this is by hacking the email accounts of law firms, then sending an email from that account to the purchaser just before the settlement date. The email asks the purchaser to transfer the money for the property into the fraudster's account.

Fraudsters will also impersonate other participants involved in the purchase like conveyancers or real estate agents – sending an email from their account that instructs the purchaser to change the type and/or location of a payment. The email may be followed up with a phone call to add legitimacy. The money is then deposited into the fraudster's account, which is quickly drained.

The tax email scam.

This is a very popular scam during tax season in the U.S. It works much like the past-due invoice scam, only instead of posing as a vendor with a past-due invoice, the fraudster impersonates the company's payroll service. The email states that copies of all employees' tax information are needed immediately so that their tax refund forms can be sent out.

In New Zealand, fraudsters can create emails that look like they are from the IRD. These usually claim that the recipient is due a refund and directs them to a website where they may be asked to enter their bank account details in order to receive the refund. We have also seen other types of IRD scams appearing around financial year end.

The gift cards for clients scam.

This newer type of business email compromise scam is very popular around the holiday season. The fraudster impersonates the victim's boss and claims to be in urgent need of gift cards for very important clients. The victim is instructed to drop what they are doing, purchase hundreds or thousands of dollars in gift cards, and email the card codes to 'the boss' ASAP.

In the future, faster payments will lead to faster fraud.

At the moment, payments take time to process, which helps us detect and prevent fraud. But due to customer demand, real-time payments will become standard in the future. With real-time payments, once the money's gone, the chance of recovery is low. This means authenticating your payment requests before they are made will become even more important.

Top tips to protect your business.

Teach your team to recognise the red flags in their inbox.

- The email contains a **request to change accounts**.
- The payment request comes through at an **unusual hour**.
- The payment request is **urgent**.
- Your staff member **doesn't know** the person who has made the payment request.
- The email asks your staff member to **click a link** and log into their account.
- The sender's name is correct but the **email address** is slightly different.
- The payment request is from a **new supplier**.
- The payment request is for an existing supplier/client to a **new bank account**.
- The payment is to a **non-New Zealand** bank account, PayPal or Western Union.
- The sender may claim to be **difficult to contact** and request email contact only.

Review how your organisation handles email instructions for payment.

Increasingly we are seeing organisations choosing not to rely on email instructions. If your organisation does rely on email instructions, consider whether your controls around payments would successfully defend against these fraudulent payment requests being actioned. These could include introducing

2 **Source:** westpac.co.nz/rednews/business/foiled-business-invoice-scam-prevents-50k-transfer

policies like dual payment authority, payment limits and daily reconciliation. The sooner you recognise potentially fraudulent activity, the better your chances of stopping or recovering from it.

Confirm email addresses.

In some cases, fraudsters can mask an email address to make it look like it's coming from inside your organisation. This can be detected by hovering over it or hitting reply which will reveal the actual email address. Fraudsters will also use lookalike domains to try and fool your staff – for example using cornpany.com as a lookalike domain for company.com.

If any customer or supplier requests a payment change by email – pick up the phone and call them.

Remember the fraudster may change the contact details on the email invoice too so don't call any phone number provided in the email message. Instead, call the employee using the number listed in your organisation's internal employee directory or look up your customer or supplier's number on official channels or even the White Pages. It sounds like a lot of extra work, but if it stops you losing large sums of money it is a worthwhile phone call to make.

Evaluate payroll information update processes and internal controls.

Think about how changes to payroll are currently made within your organisation. Carefully review and adjust your existing processes to ensure they are most effective. Make it mandatory that before any direct deposit is changed, the requesting employee is contacted directly using an official communication method.

Revisit your IT security to understand the level of vulnerability.

Consider investing in software that detects phishing emails and implement email security measures. Use software, spam and phishing filters that automatically scan emails and email addresses for spam and "spoofing" emails. It's well worth the money if you can afford it. If you're a smaller business and not wanting to spend that money, then focus on educating your people.

Make employee training mandatory.

Hold regular fraud training that covers security and cyber awareness to keep the information fresh in your employees' minds. These sessions should help employees learn to recognise and react appropriately to phishing and spoofing emails, as well as other email and phone fraud schemes. As your products and services evolve, fraudsters will look for new opportunities to attack, so make sure your advice is kept up to date.

Encourage your team to speak up.

Introduce policies like "if in doubt, call it out" to help staff feel comfortable about pointing out discrepancies or speaking out when something just doesn't feel quite right. Reward good call outs and responsible behaviour. If appropriate, create a page on your intranet where staff can share their scam stories.

Change your view of efficiency.

Everyone is trying to be more automated and efficient, but teaching your people to evaluate every email or payment request with a critical eye could end up saving your business a lot of money down the line.

Stay up-to-date.

Find out about common threats to businesses by visiting **cert.govt.nz/business/common-threats**, **netsafe.org.nz/identifying-and-preventing-business-email-compromise** or follow the Westpac NZ Facebook page for regular updates from our Financial Crime team.

New Zealand Police have partnered with Europol to develop nomoreransom.org. This online tool provides businesses with free advice on the latest ransomware threats, and step-by-step instructions to follow if you've been hacked and fraudsters are demanding a ransom to unlock your device.

Report all types of financial crime.

If your business has fallen victim to financial crime, it's important to tell us about it as soon as possible. That way we have the best chance of attempting to recover your money. We also strongly recommend that you report the incident to the appropriate authorities. They'll be able to provide advice and use the information to help prevent future attacks.

- Contact your **Relationship Manager**, local branch or our call centre if you're a Westpac customer.
- If you receive what appears to be a phishing email in the Westpac brand, forward it to **phishing@westpac.co.nz**.
- File a **police report**.
- Report scams and fraud to **Netsafe**.
- Report cyber security incidents to **CERT NZ**.

GTS10236-0620