Being alert to scams

Scams targeting builders and tradies are sadly all too common. In one recent example, a construction firm's client was targeted by a scammer informing them that the company's bank account had been changed and payment was to be made to a new account. This tactic is just one of the thousands of scams affecting businesses in New Zealand today.



Scams can surface in many guises – over the phone, via email or other forms of online communication, or even in person. To reduce your chances of experiencing any kind of scam incident, everyone in your business needs to be aware of the risks and commit to safe practices.

In the case of the change of bank account scam, precautionary practice would have been to verify this change by contacting the company - using a credible phone number – to ensure this change was legitimate. Ensuring your staff and customers are aware that this should be standard practice to carry out this simple check can help combat this kind of fraud.

Protect yourself and your business

Keeping your devices and software up-to-date is one of the most effective things you can do to keep your system safe. You need to make sure your devices are still supported by the manufacturer, and get software updates (patches) for their operating systems. Ensure you install any patches to the operating systems as soon as they're available.

Patches aren't just about adding new features to software, they often fix security vulnerabilities too. Attackers could use these vulnerabilities to gain access to your system. Installing patches that fix them is a simple way to prevent this happening.

No matter how big or small your business, make sure you educate yourself and your staff on scam threats – from the simplistic through to the more sophisticated – with regular check-ins, reading up on resources and keep doing your research.

Consumer protection NZ offers these 'eight things you can do to avoid being scammed':

1. **Be suspicious**
2. **Don't trust unexpected contact**
3. **Do your research**
4. **Resist demands to act quickly**
5. **Keep your computer virus protection up to date**
6. **Never open attachments or click on links in emails if words or images make you feel unsure about the sender**
7. **Use different passwords for logging in to online services**
8. **Reserve the right to be impolite**

Online threats

More complex and hard to detect scams, fraud or threats online come under the banner of cybercrime. Cyber security attacks on businesses are becoming more common, with the protection needed to outwit online criminals more advanced than ever. Protecting your data, network, customer information and reputation can be aided by ensuring software updates are installed, implementing two-factor authentication (2FA), backing up your data, and setting up logs. These are all good practice when running any sized business in 2023. Regardless of whether a threat is online or off, though, there is one step that is often overlooked – creating a plan for when things go wrong.

When are you most at risk?

Recognising when you're most at risk to scammers immediately reduces your vulnerability. Consumer Protection NZ says, "It's true that unexpected contact is the most common delivery method for scams, but you can also be targeted by a scammer who knows something about you. Someone running a scam may have found out more about you online than you are aware, picking up on what's happening in your life, which bank you use and what you're looking for online. We are most vulnerable to scams that make sense in the context of our lives."

Scammers take advantage of the fact that many of us look online to find work, clients or employees, as well as do our banking, our buying and run our systems online. "It can feel like a negative approach," says Consumer Protection, "but it's important to be suspicious to keep yourself safe, as scams became more difficult to spot."

Make a plan, just in case

Make sure you are alive to scam and security threats to protect your business.

- ✓ Ensure your staff and customers are aware of potential threats
- ✓ Educate yourself and your staff on the latest scam tactics
- ✓ Always encourage staff to speak up if they encounter any suspicious activity
- ✓ Have a clear point of escalation for everyone in your company
- ✓ Ensure they know when to recognise and raise a red flag
- ✓ Create a process that works for you and your business size and needs then add this to your incident response plan

Encourage staff and clients to use a separate channel of communication to verify a transaction or change before they act on it. For example, if you're doing business over email, follow up with a text message or phone call.

Online threats may come in the form of unusual email addresses. Often bogus email addresses are similar to a legitimate address but have characters missing, letters replaced with numbers, or have additional characters, such as underscores. Spelling mistakes can also be a warning sign that something isn't quite right.

If you manage to avoid a scam, share this with others to alert them to the threats. Staying abreast of scam trends and helping build awareness around them can not only prevent others from falling victim but can also create goodwill towards your business – you share because you care.

With all the best will in the world, sometimes even the most scam-savvy people get caught out. There is no shame in this. It says more about the criminals than it does about those who have been duped. Despite all the trends, technology, checks and balances, sometimes scam-busting can be as simple as pausing to listen to your gut instinct – if something doesn't feel right, chances are it isn't.

FOR MORE INFORMATION SEE:

DOWNLOAD GUIDES & MAKE A PLAN
www.cert.govt.nz

RECOGNISE AND AVOID SCAMS
tinyurl.com/scamwatch-nz

