



As a company director and an active investor in multiple national and international start-up businesses, I understand the importance of account security for your business. Over the years I have developed an effective set of strategies to safeguard against invoice fraud. I would like to share some of these with you.

Fraudsters could be trying to steal money from your business as you read this sentence.



There are three reasons you should be concerned for your business when it comes to account security. Firstly, in New Zealand we have a pretty relaxed outlook on life and that includes security. Secondly, there is a lot of money to be made from cyber fraud, and finally, it's very difficult to get caught.

We are all reliant on information technology, and we want to be able to trust that our accounts are safe. That's why I like to use a "four pillars" approach to security, as follows:

1. Governance
2. Policy
3. Prevention
4. Recovery

I would like to walk you through what these steps look like, and how you can use them to protect your business from invoice fraud.



Here is a very quick summary:

1. Governance: Good governance that exposes risks to the top table of your business
2. Policy: Effective policy that engages your staff, encouraging them to become more security aware
3. Prevention: Good technology that prevents most of the nasty stuff getting in, but is in no way fail safe (this is what many in the industry will be trying to sell you)
4. Recovery: The ability to recover your business as quickly as possible if you are in any way compromised

This next little gem fits very neatly under our “policy” pillar. One very simple way that you can considerably minimise this risk is through much tighter bank account matching.

Sharpening up on your policies around bank account changes will add an additional layer of security that is difficult to compromise.

Before we look at preventing invoice fraud, we need to understand it.

Invoice fraud is all about convincing you and/or your staff to reroute payment to the fraudster. To do this they need to study your business, learn your patterns, and sometimes engage with you in order to probe for weakness.

You should never underestimate how much time and effort they will put into this. Sophisticated fraud attempts can be very difficult to spot.

Once payment is made, the money is gone. There is generally nothing your bank, or the police, can do about it.

It is a huge issue in New Zealand, and one that simmers under the surface. Many fraud attempts are unreported, or go unnoticed - until it is too late.

That's why having a good plan in place is paramount.

“Four pillars” is a strategy to deliver a relevant and practical “whole of business” approach to secure your business.



Bank account numbers should be carefully and actively matched.

This applies to your clients, creditors and the like. In nearly all cases they should be New Zealand bank accounts.

Alarm bells should always ring when there is an instruction to change a bank account, or you receive an invoice with a non-matching account number.

There should always be a mandatory policy with associated process to follow. This could include a contact process (itself not always foolproof), a verification process that may include some sort of challenge or response, an analysis of the bank account number itself, and an internal sign off or workflow process.

In essence, you need a healthy dose of scepticism associated with any change, and a policy framework that supports this.

Taking your time to verify these changes will add a bit of overhead, but we warrant it will impress your business partners. However, and most importantly, it is a simple but effective policy step towards becoming “four pillars” cyber-secure.



Please feel free to contact us if you would like assistance with this, and share this with anyone who may benefit. We would love to hear from you if you found this article useful, or if you have anything you have done that we could share with our community.

For more information on how to spot and prevent scams, go to:

- www.consumerprotection.govt.nz/get-guidance/scamwatch
- www.netsafe.org.nz/fake-invoice-scam/
- www.business.govt.nz/news/protect-your-email-account-from-invoice-scams/

Phil Johnson
OneLaw Director, and Independent Business Consultant
Expert on the intersection of technology and law
Available for speaking engagements or consultation

Email: nzphil@icloud.com

Phone: 021 322 718

Find Phil on LinkedIn

