ONLINE FRAUD PREVENTION ACTION PLAN

PAYMENT ASSURANCE

Ensure that documentary evidence is kept detailing all payee bank account details. This could include: an invoice that has the details printed on it; a copy of a deposit slip; or an email directly from the payee confirming their bank account information.

Actioned by ***Completion date***

Regularly spot check payee account details you have recorded in your online banking software against those provided by your creditor.

Actioned by ***Completion date***

To maximise security and privacy, restrict access to the directories where accounts payable, accounts receivable, or payroll files are saved to.

Actioned by ***Completion date***

Periodically complete independent/external audits of your bank accounts.

Actioned by ***Completion date***

Complete regular reconciliation of your bank accounts.

Actioned by ***Completion date***

Regularly audit your business processes to ensure your financial affairs are being managed as you had intended.

Actioned by ***Completion date***

Review whether your business insurance is sufficient to protect you from fraud.

Actioned by ***Completion date***

SOFTWARE ACCESS

Actively manage the services and access that you delegate to your staff through your online banking software – ensuring you only assign the access staff require to perform their role.

Actioned by ***Completion date***

If your business uses accounts payable/receivable or payroll software, regularly review who has access to these systems.

Actioned by ***Completion date***

Wherever possible have two authorisers approve all payments. Additionally, investigate whether your business would benefit from using Second Factor (2FA) devices to authorise payments.

Actioned by ***Completion date***

Delegate the ability to authorise payments to staff other than those who can create and maintain payees or payments.

Actioned by ***Completion date***

For staff that have the ability to authorise payments, individual dollar limits can be assigned to each of them, restricting the maximum amount they can approve at any one time. Review these regularly to ensure they are in line with the needs of the business.

Actioned by ***Completion date***

PASSWORD SECURITY

Ensure that you have a robust policy around password maintenance and strength within your business. You may want to consider requiring that:

- Passwords are changed regularly
- Passwords are not something easily guessed by others (e.g. pet names, birthdays etc)
- Passwords contain a mixture of upper case, lower case and special characters
- Passwords do not contain ascending, descending or repeating sequences of characters or numbers

Actioned by ***Completion date***

On a regular basis, review who within your business has the ability to change the passwords of other users in both your online banking software and any accounts payable/receivable or payroll systems you use. A number of systems are able to produce audit log reports of administration activity, and where possible, these should be periodically reviewed by an independent party.

Actioned by ***Completion date***

Make sure all your staff know they must take appropriate steps to ensure their password is not known to anyone else. There are no circumstances under which any user should disclose their individual password to anyone, including to the administrators of your banking software.

Actioned by ***Completion date***

Ensure staff are aware never to respond to emails asking for personal or business banking access names or passwords, a practice known as “phishing”. The government’s Scamwatch website located at consumeraffairs.govt.nz/scams has useful advice in this regard.

Actioned by ***Completion date***

Do not attempt to access online banking from publicly accessible computers where keystroke logging or virus software may be installed without your knowledge (e.g. internet cafes).

Actioned by ***Completion date***

Do not attempt to access online banking services using free WiFi internet hotspots from your own laptop or tablet. When using these services, your internet access could be monitored and access details intercepted.

Actioned by ***Completion date***

NETWORK SECURITY

Make sure your computers have up-to-date anti-virus software installed.

Actioned by ***Completion date***

Install an appropriate protective firewall for your business network.

Actioned by ***Completion date***

Periodically scan your workstations for spy-ware or keystroke logging software.

Actioned by ***Completion date***

Educate your staff about Internet usage risks:

- The dangers of clicking on pop-up advertising
- Downloading free software from the Internet
- Understand what adware, malware and spy-ware are

Actioned by ***Completion date***

Devices that are shared, or are connected to many computers e.g. smartphones, music players, USB memory sticks can also be a mechanism for spreading viruses and spyware. Ensure your business has a robust policy around what devices can be connected to your network, and how they are being monitored.

Actioned by ***Completion date***

If you are concerned you have been a victim of online fraud or note anything of concern, ring us immediately on 0800 240 000 or +64 4 801 2400 from Overseas (international toll charges apply).