Secure your business website

Unsecure websites are vulnerable to attack. Keep your business and customer information safe by working through the steps on the checklist below.

Steps to work through yourself:

- □ **Create a long and strong login password** for your website that is different from any used for other services. We recommend a passphrase of four or more words.
- □ **Turn on two-factor authentication (2FA).** 2FA verifies you are who you say you are, by asking for a second piece of information (often a code) as well as your password. This adds an extra layer of security.
- □ **Keep your software up-to-date.** This includes your content management system (CMS), any plugins or external modules you use, and other items such as your web server.
- □ **Back up your business data regularly.** Set the backups to take place automatically and store them somewhere secure, but easy to get to, such as a locked drawer or cupboard, preferably offsite. Having backups means you can restore your data quickly and easily if it's lost, leaked or stolen.
- □ **Create an incident plan** to guide you if something goes wrong. This should include the contact details for your IT and communications support people. Having a plan will help you minimise the impact of an incident and get back on your feet quickly.
- □ **Report cyber security incidents to CERT NZ.** They can advise you on next steps. The information you provide will also be helpful in creating preventative advice for others.

Steps to work through with your IT provider:

- □ **Enable HTTPS on all pages,** including on your CMS, where you make changes to your website.
- □ **Set up to receive alerts** when someone makes changes to the website or CMS.
- □ **Check your CMS** periodically to make sure the 2FA and alerts are still configured correctly.
- □ **Follow cyber security best practice** when making changes to your website. Ensure your website developer or IT support follows the cyber security techniques outlined in OWASP.
- □ **Check you still need all the plugins** installed on your website. If you don't need them anymore, remove them – they make your website an easier target for attackers.
- □ **Get Payment Card Industry Data Security Standard (PCI DSS) compliant.** PCI DSS helps ensure that online transactions are safe and secure, and that customers' card data is protected from attackers. Your bank requires your online trading website to be PCI DSS compliant, so talk to them about what's involved.

  You're strongly advised not to process any online payments yourself. Use a third party payment gateway provider who is already PCI DSS compliant.

Find out more at
www.cert.govt.nz/business

New Zealand Government