Protect your website from online attacks

The current uncertain business climate demonstrates just how important your website is to your business. Given the need to boost your online presence and increase your online trading, it would be understandable if website security has taken a back seat. Your website contains business and customer information that is valuable to cyber attackers, so it's worth taking the time to safeguard it.

As part of their current 'Trade Smart Online' campaign, our friends at CERT NZ have provided some practical steps you can take to keep your website safe and secure. You'll be able to do some things yourself, while you might need an IT-savvy friend or IT provider to lend a hand with the others.

The four priority measures to get underway now are outlined below. The full list of steps to protecting your website is available at: www.cert.govt.nz/protect-it

1. Secure the data on your website

Your customers trust you to keep their information, and the communication you have with them, confidential and safe. An easy way to give your website added security and privacy is to enable HTTPS across your entire site. HTTPS keeps the information transferred between you and your customers confidential by encrypting it. This stops attackers from getting the login details or credit card information customers submit on your site. HTTPS should be enabled across your entire website.

2. Update software and devices

Running a business is hectic. There's so much to remember and keep track of – from payroll to sales and purchase transactions and stock control. Give yourself one less thing to think about by automating as many tasks as you can, including updates. Updates not only add new features, they fix issues or vulnerabilities that allow attackers to get the valuable information on your website.

As the business owner, it's your responsibility to make sure your website's software is updated and any security patches are applied.

3. Get PCI DSS compliant

If you trade online, you'll want to get up to speed on the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS helps ensure the online transactions on your website are safe and secure, and that your customers' card data is protected from attackers. Being PCI DSS compliant means you're well-placed to avoid a security breach that can result in loss of revenue, customer trust and reputation.

Most banks require PCI-DSS compliance for any site accepting online payments, so talk to yours about what's involved.

ANZ:	www.anz.co.nz/business/products-services/merchant-services/security-pci/
ASB:	www.asb.co.nz/business-banking/pci-dss-protecting-payment-card-information-guide.html
BNZ:	www.bnz.co.nz/business-banking/support/merchant-services
Kiwibank:	www.fetchpayments.co.nz/help/pci-dss-compliance-guide/
Westpac:	www.westpac.co.nz/business/payment-solutions/security-and-information/

Find out more about PCI DSS and safely operating an e-commerce site safely here: https://www.cert.govt.nz/business/guides/secure-your-website/accepting-payments-online

4. Renew your domain

When you registered your domain name you obtained a licence to use that name for the registration period, but you don't own it. If your domain licence were to expire an attacker could claim it and set up their own scam website selling fake goods or serving malware using your business' name. Keep your domain yours by making sure your registration stays current. Ask your domain provider about auto-renewing your domain.

Read the Domain Name Commission's advice about domain name registration here: www.dnc.org.nz/sites/default/files/2016-02/a_ready_reference_for_registrants.pdf

Report it

If you think your business might have experienced a cyber security incident, report it to CERT NZ.

CERT NZ is New Zealand's Computer Emergency Response Team, and works to support businesses, organisations and individuals who are affected (or may be affected) by cyber security incidents. CERT NZ provides trusted and authoritative information and advice, while also collating a profile of the threat landscape in New Zealand.

Report a cyber security issue to CERT NZ here: www.cert.govt.nz/individuals/report-an-issue/