Protect your website with our top ten tips checklist

There are several things to do to keep your website safe, below we've provided the top ten tips to keep your website secure. You can use the list below as a checklist and they'll help keep your website, and your customer's information, safe and secure:

- [ ] Make sure your login **password is long and strong** and different from any other service you use.
- [ ] **Turn on two-factor authentication** if it's available. This adds a second layer of security, by asking for a second action (often a code) after your password to check you are you.
- [ ] **Keep your software up-to-date** – this includes your admin section, any plugins or external modules you use, and any other areas you look after (e.g. your web server).
- [ ] **Create an incident plan** for what to do if something goes wrong, including your key contacts for IT and communications support. The plan will help you minimise the impact and get back on your feet.
- [ ] If you have a security incident, **report it to CERT NZ** so they can advise you on your next steps. They'll also use the information to create preventative advice for others.

You may need to work with your provider to complete the following security tips:

- [ ] **Enable HTTPS on all of your pages**, including on your admin panel where you log in to make changes.
- [ ] **Set logs up** and get them emailed to you. These record when someone accesses the content management system or changes the files.
- [ ] Occasionally **check the logs** are still working as they were set up. Once they gain access, attackers often turn the logs off so that you won't be able to track them.
- [ ] If you make changes to your website, **follow security best practice** – ask your developers or IT support provider to follow the security techniques called OWASP.
- [ ] **Check you still need all the plugins** you have installed on your website. If you don't need them anymore, remove them. They're easy targets for attackers.