**KAREN STEPHENS**

Karen is CEO and co-founder of BCyber, an agile innovative group who works with SMEs to protect and grow their business by addressing their cybersecurity and governance risk gaps by demystifying the technical.

# Ten top tips to secure your website

In May this year Domain.com.au advised that a cyber-attack had resulted in an unauthorised third party gaining access to users' personal information and deposit details. Yet, when you mention cybersecurity most people automatically think of antivirus, the Deep and Dark Web, Ransomware as a Service, and possibly the need for a cyber awareness program or endpoint protection. Few people, if any, have website security top of mind.

Website attack is very popular with the cybercriminals. Some estimates put attack numbers as high as 50,000 websites per day. The cybercriminals tend to adopt a "spray and pray" approach, using programs that detect websites with accessible vulnerabilities, only a small minority target specific sites. Cybercriminals do not necessarily want your data. They may want to use your server as an email relay for spam or set up a temporary web server for nefarious purposes, plant malware, redirect traffic to another site to name but a few objectives.

You can implement a few small, but powerful measures to protect your website.

1. **Review your site security.** Have a formalised scanning and review program covering access levels, patching, updating protocols and the like.
2. **Take ownership of security.** Do not leave the security of the site in the hands of the wrong people, for example marketing or web designers. They may be great at what they do, but would you let your interior decorator recommend, implement, and monitor your back-to-base alarm?
3. **Implement least-privilege access.** Limit people's access to the lowest level they need to do their job. Not everyone needs full admin access. And limit external parties' access and timeframes. There is no need to have umpteen administrators. People with unnecessary access can result in unwanted website security incidents and when a staff member leaves, check that their website accesses are removed.
4. **Deploy a secure sockets layer (SSL) certificate.** Buy an SSL certificate. With that little lock showing in the top left corner of your website you boost your SEO rankings and ensure any data your visitors send to your site is using an encrypted channel, so cybercriminals cannot see it while it's in transit. You may even wish to consider upgrading to TLS (Transport Layer Security) a more recent version of SSL.
5. **Update early, update often, update everything.** Websites use tools to run effectively: content management systems, plugins, WordPress, Java scripts and the like. Updates not only fix "bugs and glitches", but they also often provide security enhancements. Updating immediately means you are closing a vulnerability and remaining one step ahead of the cybercriminals.
6. **Have a website backup strategy.** A regular backup program will help you recover more quickly from a site hack (or human error or an update problem). Ideally you should have the backup stored on a server other than the one hosting your website. You do not want to lose your website only to find your backup has been infected as well, because that would mean a full site rebuild.

7. **Practice good password hygiene.** Keep your admin passwords safe and choose complex passwords with at least 12 (some say 16) random characters, including upper and lower case letters, numbers, and symbols. Never reuse passwords. Never share passwords, and never use any personal details in your passwords (social media is a fount of information for the cybercriminal).

8. **Change default settings.** This includes even those without an obvious security focus. Do not allow the cybercriminal into your settings so they can leave the gift of malware. Some settings you may wish to consider changing include user controls, file permissions, comments settings. And please customise the WordPress admin login URL.

9. **Do not make it easy for the cybercriminal.** Never use admin, or test, or backup, or your site's name as the username for your administrator account.

10. **Invest in and install web security tools.** Plugins and Web Application Firewalls (WAFs) are easy to source and not that expensive. They harden your site security posture and can monitor for malware and viruses.

BCYBER®

Remember BCyber. Be cyber safe.

*If anyone would like a little website security help they can book a meeting with us (Book a meeting with BCyber) and we can run a security and marketing review report for them and discuss how they can harden their websites..*

in *www.linkedin.com/in/karen-stephens-bcyber/*

W *www.bcyber.com.au*

E *karen@bcyber.com.au*

*twitter.com/bcyber2*

*youtube.bcyber.com.au/2mux*