MATTHEW FORD, *Total Web Solutions Perth*
Website: totalwebsolutions.com.au
Small businesses and sole traders need responsive suppliers who understand how they work and when support is needed. Total Web Solutions is all about peace of mind, providing professional, secure website design and development services but with that personal touch. Services include cloud hosting, SEO, SEM, and technology and security support. Matthew has a background in technology and engineering, has been building websites for over 15 years and would like to give your small businesses a big voice.

TIP 1. KEEP WEBSITES PATCHED AND UP TO DATE

Like phones and laptops, websites run on layers of software that need to be kept up to date such as PHP, WordPress, plug-ins and themes. A well patched website will help protect you from hacking attempts, and help ensure optimal website performance. Websites should be monitored and regularly updated, which is a service usually provided by your website developer that would include backing up the site before making any changes.

TIP 2. PASSWORDS PROTECT

Use strong passwords everywhere, and don't use the same passwords in multiple places. Even better, use at least two factor authentication (2FA) to ensure only authorised users have access to your personal information and systems. Build up layers of security by using 2FA on all of your points of entry including: desktops, laptops, mobile devices, websites and email.

TIP 3. BE WARY OF EMAILS AND SMS MESSAGES

Email and text messages can contain links or images that look legitimate and appear to be from your bank or email provider, for example. These are often used to harvest email addresses, user names and passwords that will then be sold or used in hacking attacks. This process of sending fake emails and messages is commonly known as 'phishing'. Also try to avoid using email and SMS messages as a part of your security system. Your cyber security framework is only as strong as its weakest link.

TIP 4. ENSURE YOUR WEBSITES ARE BACKED UP REGULARLY

Back up everything, and back it up regularly. Also, occasionally check that your backup systems work as intended. When things go wrong, and they sometimes do, having a good backup can be the difference between having your website down for weeks and having to rebuild from scratch, or just having your business offline for a few hours with some possible repair work to complete.

TIP 5. ENSURE YOUR WEBSITE HAS AN SSL CERTIFICATE

SSL (Secure Sockets Layer) certificates are used to keep website data secure and to give users confidence that your website is going to protect their personal information. It ensures that data is encrypted between users and websites, therefore preventing hackers from intercepting the data. Google is pushing SSL hard, and highly prioritises websites with SSL certificates above those that don't. Check to be sure your website address starts with HTTPS:// rather than HTTP:// which is insecure.

TIP 6. DON'T BE AFRAID TO ASK FOR HELP

It's great to get involved, to research and learn from reputable sources. But we can't be an expert in everything. If the stakes are high, stick within your areas of expertise, and bring in experts in other fields when required.

TIP 7. NEVER SHARE PASSWORDS

Every website user should have their own unique user name and password. There are two parts to this, the first being of traceability and accountability of what happens under each user name, and the second being the many insecure ways that passwords are usually shared.

TIP 8. PROTECT LOGINS AND CONTACT FORMS FROM BOTS

Consider the use of CAPTCHA at online entry points to stop bots (short term for 'robot') from logging in and creating spam accounts. These spam accounts are not just annoying, they can also contain malicious or unsavoury links and text. Using CAPTCHA on website contact forms is also highly recommended as it helps to stop bots from sending emails with potentially malicious content like phishing scams to you or your team via your own website.

TIP 9. ENSURE YOUR WEBSITES ARE PROTECTED

Sometimes it pays to add an additional layer of security. I recommend all my clients use a web application firewall to help protect their website from malicious traffic, malware, brute force attacks and known threats. There are many different types of software available, with varying degrees of protection and quality - so be sure to do your research, or have a chat with your website developer.

TIP 10. HOST YOUR WEBSITE SECURELY

Hosting is essentially the computer on which your website runs. This computer needs to be kept up to date and should run the latest versions of server software to help protect your website and its server against hacking and unauthorised entry, but also to ensure that your website is as stable as possible with minimal downtime. Unless you host your own website your website developer will usually look after this for you.