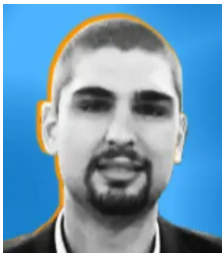

PAUL IOPPOLO - *Founder/Director - Perth IT Care*
Website: https://www.perthitcare.com.au/

Paul is an experienced IT professional with over 16 years of real-world expertise, he is the founder and director of Perth IT Care. This specialised IT and web business focuses on hacked website recovery / repair and small business IT solutions. With a dedicated commitment to micro and small businesses, Paul establishes robust connections across Australia to provide essential protection and support. By fostering relationships with these entrepreneurs, he empowers the "little guy" to safeguard their digital assets and establish a secure online presence.

TIP 1. UNDERSTANDING THE IMPORTANCE OF YOUR DOMAIN'S SECURITY

To ensure effective website and email security, prioritise domain protection. Neglecting it poses vulnerability, especially without sufficient knowledge, as user error contributes to disruptions. Don't buy domains based solely on cheap prices from random sites. Find a trusted provider offering domain sales and management. Neglecting domain security risks unauthorised access to your platforms, endangering clients with potential phishing.

TIP 2. EXPIRED DOMAINS ARE STILL A HACKING RISK

When a domain expires, it's crucial to ensure that it is not linked as the security email for another domain, especially your main domain. If someone acquires the expired domain, they gain control over the security transfer rights for your other domain. With the successful transfer of your domain, they can redirect your website to a phishing site, impersonate you to your clients and other contacts and (in the worst case) compromise your email platform allowing them to perform a man in the middle attack

TIP 3. BE CAREFUL WHO YOUR EMAIL PROVIDER IS

When choosing an email provider, prioritise their reputation and security capabilities, encompassing features like 2FA(Two Factor authentication), malware protection and spam protection. Accurate configuration of these settings is crucial for their effective operation. Remember, your email provider has access to your content, so make sure you can trust them.

TIP 4. WEB HOSTING SUPPORT MATTERS

When choosing a hosting provider, it's crucial to make a thoughtful decision because you'll heavily depend on their support in two critical instances. Firstly, during website setup, and secondly, in unfortunate events like security breaches. If your website is hacked, you might find yourself relying on an offshore call centre support to rectify the issue and restore functionality. The longer the recovery process takes, the worse the impact can be.

TIP 5. ONLY USE A CMS IF YOU PLAN ON MAKING FREQUENT CHANGES TO YOUR WEBSITE

CMS (Content Management System) platforms like Wordpress, while providing convenience for website management, can be vulnerable to compromise. They offer a user-friendly interface, but unfortunately, they often become significant weak points in terms of security. If your website doesn't require frequent updates, it may be worthwhile to consider a non-CMS website. By eliminating the CMS, you significantly reduce the potential surface area for hacking attempts,

enhancing your website's overall security.

TIP 6. IT'S NOT ALWAYS A PERSON IN A HOODIE AT A KEYBOARD TRYING TO HACK YOU

Your personal information holds value and can be sold to others. Many hacking attempts are automated scripts designed to target hundreds, if not thousands, of websites. Your website is not singled out as special; it faces the same level of risk as any other.

TIP 7. BE CAREFUL WHERE YOU ARE GETTING YOUR ADVICE FROM

It's common to encounter individuals who claim to have some knowledge about various subjects and are eager to offer their opinions. However, when it comes to cybersecurity, it's crucial to seek advice from true experts in the field. Relying on the expertise of cybersecurity professionals ensures that you receive reliable and accurate guidance. It's important to prioritise the insights of those who have extensive knowledge and experience in cybersecurity to make informed decisions and effectively safeguard your technology.

TIP 8. UNLESS YOUR WEBSITE IS BRAND NEW, THERE IS ALWAYS SOMEONE ACTIVELY TRYING TO GET IN

Unless your website is freshly created, it's important to recognise that there are always individuals actively attempting to breach its security. Cybercriminals continuously scan the internet for vulnerabilities, utilising automated tools to identify potential targets.

TIP 9. BY DEFAULT, WORDPRESS LACKS SUFFICIENT SECURITY MEASURES IN ITS BASIC SETUP

WordPress exposes crucial information during the login process: confirming the correct username but incorrect password, inadvertently disclosing half of the login credentials. It reveals the software version, PHP version and the username of the page creator, all of which can be exploited by malicious actors to launch targeted attacks and gain unauthorised access.

TIP 10. RESEARCH THE THEMES OR PLUG-INS YOU ARE ADDING TO YOUR WORDPRESS SITE

Creating a theme or plug-in is open to anyone, but if not developed correctly, it can introduce vulnerabilities that can be exploited. What's even worse is that a theme or plug-in can be intentionally designed to compromise the website it's installed on, and potentially even other connected websites.