MARTIN BOYD *- CEO and Founder, Vertex Cyber Security*
Linked In: https://www.linkedin.com/in/iammartinboyd/

Martin founded Vertex Cyber Security in 2016 with the mission to protect Australian businesses and families from cyber harm. He has over twenty years of experience in the technology industry, including as Executive Manager Cyber Security at CBA. He is genuinely passionate about making cyber security accessible and affordable for all organisations. He has recently accepted a role on the Board of Directors for CREST AU/NZ, an accrediting body for cyber security providers in Australia.

TIP 1. A GREAT PASSWORD MANAGER IS WORTH IT'S WEIGHT IN GOLD (BUT WON'T COST YOU THAT MUCH!)

Password security is critical to robust cyber security. It can also be incredibly frustrating trying to remember unique passwords for every system or platform. People are often concerned about storing their passwords in a Password Manager however options like BITWARDEN are incredibly secure, affordable and make managing your passwords (including shared passwords) simple!

TIP 2. A LAYERED DEFENCE IS THE BEST DEFENCE (YES, WE'RE TALKING 2FA!)

With the prevalence of phishing attacks, and in a world of constant data breaches, strong passwords are not always enough. Multi-factor authentication (or 2FA) should be enabled wherever possible. Physical security keys with FIDO2 (like the YUBIKEY) are your best option, but Authenticator apps are better than no 2FA.

TIP 3. DON'T FALL BEHIND WITH YOUR PATCHING

Patching (or applying security updates) to your operating systems and software is a simple but important step to take in protecting against known vulnerabilities which might exist in the application. We recommend allowing automatic updates on your devices and having a process in place to apply updates as soon as they become available. It's not just about software fixes, but often new security features are also included to protect your data and device.

TIP 4. EDUCATION IS HALF THE EQUATION

Accessing simple, practical and engaging cyber training resources is a great way to ensure you and your team know what the risks are, and how to best manage them. Vertex offers online Cyber Awareness training for teams and covers topics including phishing, workspace security, business email compromise and more. Use the coupon code BBECCYBERSAFE to receive a 3 month free trial at https://auth.vertexcybersecurity.com.au/signup/.

TIP 5. DON'T JUST CLICK 'CONNECT'

Free or public Wi-Fi networks can put your information at risk and expose your data and logins to cyber criminals. Using trusted Wi-Fi connections is key. Use your password encrypted home or work internet or mobile data service. Otherwise ensure you have set up a Virtual Private Network (VPN) to connect through – EXPRESSVPN is just one of the many options available.

TIP 6. PHISHING ATTACKS ARE STILL A BIG DEAL

Phishing attacks remain one of the most effective methods used to compromise businesses in increasingly sophisticated attacks. XSURFLOG is a Vertex product which acts as a last line of defence, blocking suspicious links in the browser if the user doesn't identify it as a phishing email and clicks through.

TIP 7. THE OTHER TECHY STUFF IS IMPORTANT TOO

Knowing how to improve your cyber security practices can feel overwhelming and it can be difficult to know what you really need. Engaging a cyber security partner can help with prioritising the best bang for buck options. Some of the important protective measures to consider include: implementing a spam filter, hardening your email service (beyond the default settings), using anti-virus/anti-malware which includes monitoring of new software and enabling a firewall across all computers (ideally one which dynamically blocks cyber-attacks and malware).

TIP 8. BACK UP BACK UP BACK UP

Backups become critical in the event of a cyber-attack. However, it's also important that your backups are protected too. Backups should be completed regularly, stored separate to your data (e.g. at a different location) and must be encrypted to ensure they could not be the cause of a cyber breach.

TIP 9. IT NEVER HURTS TO KNOW WHERE YOU STAND

External cyber security providers (like Vertex!), see and respond to cyber-attacks across a diverse range of businesses all the time. That means that we understand the risks and protections required to safeguard your business (and livelihood). A Cyber Security Audit will identify any process or technical gaps and provide advice on how to remediate these, in line with industry best practice and recognised cyber security standards.

TIP 10. AND LASTLY, PREPARE FOR THE WORST (AND HOPE FOR THE BEST!)

Regardless of the size of your business, preparation is key. The impact of cyber-attacks can be severe, especially for small businesses and the individuals and families behind them. Having an Incident Response Plan in place is important in the event of a cyber incident as it reduces response times, in-the-moment decision making and harmful impacts. Practising the plan on a regular basis ensures your team knows what to do if an attack occurs.