SIMI DAS, *Director, Easy Start Cyber - (Certified Information Systems Security Professional (CISSP), Bachelor of Engineering in IT, MBA Candidate at UWA, Board Member)*
LinkedIn:linkedin.com/in/simidas
Website: https://www.easystartcyber.com.au

Simi has over 17 Years of international experience in technology, including IT and OT security, working for Cybersecurity product companies such as McAfee, Narus (part of Boeing) and various Perth-based companies such as Mineral Resources Limited, BGC Construction, Perenti Group, Western Power among others. Her understanding of Cybersecurity Product Development, Network Security background, and extensive expertise in Cybersecurity Governance, Risk Management, and Compliance makes her ideal to establish and process Cybersecurity Strategies for various organisations. Through her company Easy Start Cyber, she is helping Australian businesses in managing Cyber Risks and responding to Cyber Incidents.

TIP 1. YOU VERIFY AS THEY VERIFY

Many times, it is unavoidable not to answer an unknown number. If you receive a call asking you to verify your identity or financial details, make sure you verify the caller's identity first by hanging up the call and re-dialling the organisation the caller claims to be from. The call could be a potential fraud leading to identity theft.

TIP 2. WANTING MINIMAL IMPACT ON OPERATIONS FROM CYBERSECURITY INCIDENTS, THEN BACK-UP IS YOUR ANSWER

Regularly and frequently (daily or, if not possible, at least once a week) back-up your business data; including payment details, customer information, quotes, and orders, to an external storage or cloud storage and keep it safe by limiting access - setting passwords for accessing, if possible, by applying encryption. This helps quickly resume operations after a cybersecurity incident with minimal impact.

TIP 3. EXTRA STEP EXTRA SECURITY

Enable Multi-Factor-Authentication for all applications necessary for your business with 'Passphrases' (a string of words as a password) as an authenticator. Enabling Multi-Factor-Authentication is one additional step before you login to applications; however, it saves you from brute force attacks, data sniffing, and social engineering techniques and alerts any unwanted login attempts, ensuring extra security.

TIP 4. THINKING OF INSURANCE? UNDERSTAND REQUIREMENTS FOR CYBERSECURITY

Cyber liability insurance covers the cost of keeping your data secure and the expenses of any disruption to your business. The Insurance Council of Australia endorses the Australian Cyber Security Centre's Essential Eight Maturity Model as the first step towards improved cyber security health for all small to medium businesses.

TIP 5. KEEP CYBERSECURITY YELLOW PAGES UP TO DATE AND HANDY

Your business could be a victim of a cyber-attack by hacking your business email account or impersonating your business by another method. Prepare yourself for the worst-case scenario of a cyber breach. Keep your Yellow-Pages of important Contact Details up to date and handy in case you can't use your computer. Seek professional help to limit the damage.

TIP 6. WELCOME SOFTWARE UPDATES

Software updates are improved versions of existing software you're using. If it is hard to remember the schedule of software updates, then turn on automatic update for operating systems, applications, and programs. Do not hesitate to reboot where needed after the update installation. Welcoming software updates will reduce the likelihood of exploitation of weaknesses in your information systems.

TIP 7. PRIORITISE EMAIL SECURITY

Cyber attackers try to lure users into approving a fake invoice transfer request, divulging sensitive information, or downloading malicious software. To secure emails, enable encryption by installing an email certificate like Pretty Good Privacy (PGP). Configure Email authentication mechanisms such as SPF, DKIM, and DMARC that provide proof that an email message is genuine and that it's coming from who it claims to be from, preventing phishing and email spoofing.

TIP 8. MINIMISE DATA COLLECTION

Understand how your business collects customer and employee data. Only collect relevant information that your business needs. For example, there is no need to collect the medical history of a customer if it is unrelated to your business. Keep customers' personal information secure and protected from unauthorised access, modification or disclosure.

TIP 9. UNDERSTAND THE RISKS ASSOCIATED WITH GENERATIVE AI (SUCH AS CHATGPT)

Generative AI, such as ChatGPT, may help you in day-to-day work, but understand the implications of using Generative AI. Sharing information to such a model is used as training data and consumed by external entities. Refrain from providing business-sensitive information as input to such a model. Do not directly utilise the output information received from such a model in official documents without validating the quality and accuracy.

TIP 10. BE CYBER AWARE AND SEEK ASSISTANCE WHEN YOU NEED

Educate yourself, and your staff, on healthy cybersecurity habits to ensure better email security, understand social engineering, report suspicious activities leading to cyber incidents and always keep devices, applications and browsers up to date.