LESLIE RAYMENT - *Founder, NETCorp IT Solutions*
LinkedIn https://www.linkedin.com/in/leslierayment/

With 25 years of business knowledge and insight, Leslie brings his life lessons and expertise with him. He has proven to be an experienced person with defined levels of excellence and a passionate approach towards business. Complementing Leslie's rounded business experience, he pulls in 20 plus years working as an ICT professional for Perth based businesses. Continually striving to guide his clients in ways to streamline and optimise their operations by implementing sound business process practices utilising current technologies and methodologies.

TIP 1. PROTECT YOUR ONLINE ACCOUNTS

Password theft is commonplace and the need to secure your online accounts with multiple layers of security is essential. Security such as Multifactor Authentication (MFA) allows for a security measure that not only implements something you know – a password, but something you have – a smart device, and possibly who you are – a fingerprint or other biometric. MFA apps such as Google's Authenticator or Microsoft's Authenticator allow for you to also move away from emails.

TIP 2. PROTECT YOUR COMMUNICATIONS

Business Email Compromise (BEC) is on the rise as we increase smart device utilisation and adopt a transient workplace model. Education and awareness of how to detect malicious emails is as much an important aspect as ensuring you have a business-grade email filter. The move towards team collaboration tools such as Microsoft Teams, Slack and Flock allows for fast, secure team communications outside of emails.

TIP 3. TRAIN YOUR TEAM

Training your staff to understand different threat vectors (such as a phishing emails) can be a simple and cheap exercise. The Australian Cyber Security Centre (ACSC) website provides free resources to assist individuals and small businesses understand what risks are and how to avoid them. Alternatively, many organisations specialise in just this - training end users to understand various threats and compromises.

TIP 4. USE YOUR HOTSPOT

No public wi-fi is safe! It is too easy to clone, intercept, or hack into a public wi-fi and therefore it should never be used, instead use your smart device. So, when you are out and about: use your smart device. What you'll find is that your smart device has a feature called Hotspot which utilises the data on your device's cellular account and therefore can be trusted.

TIP 5. HAVE FUN WITH PASSWORDS

!Pinky & the Brain for World Domination; is a fun easy way to remember a complex password !P&tB4WD. Passwords do not have to be hard to remember, just utilise an easy to remember phrase, ensure to add capitals and lowercases, including a number and symbol, with at least eight characters long. This is an old tip but still relevant today than ever before. <<the Buck Stops With us!! <<tBSWu!!

TIP 6. YOU ARE NOT ALONE

You don't have to go it alone. Find a good ICT partner. In this, seek out a Managed Service Provider (MSP) or a Managed Security Service Provider (MSSP) as these are technology solution providers who can assist you individually, or as a team. They have the skill set to advise and guide you through your ICT requirements and associated security risks. Everyone is unique and a good MSP knows this, they'll cater to your specific needs - offering up a solution that will work for you.

TIP 7. PROTECT YOUR PII – IT'S VALUABLE!

PII stands for Personal Identifiable Information, any information that allows for a cybercriminal to identify or locate an individual. This includes, but is not limited to:- name, date of birth, address, Medicare number, bank account details, phone numbers, or in short, any physical or digital identity information about you. You should be cautious about the information you place online, such as the "always-on" Social media platforms, Facebook, Instagram, LinkedIn, and so on.

TIP 8. 3-2-1 BACKUP BACKUP BACKUP

Backing up your data is quite often overlooked and yet vital. There's a simple principle to use and that is to follow the 3-2-1 rule. That is keep 3 copies of your data on 2 different types of media (local and external hard drive) and 1 copy in an off-site (cloud storage) location. If you lose your data or fall victim to ransomware or malware you will be able to recover your data. Priceless!

TIP 9. AS WITH BACKUP – UPDATE UPDATE UPDATE

Software weaknesses - known as Vulnerabilities - are what cybercriminals look for to exploit. These are the easiest ways into a system and therefore the most common way used by a cybercriminal. Much like a home, the easiest way to break-in, is what will be exploited. Updating your systems applications and operating system with the latest patches and security fixes of known vulnerabilities removes weaknesses to provide a better level of protection.

TIP 10. REGISTER TO THE ACSC ALERT SERVICE – CYBER.GOV.AU

Individuals can register to the free Australian Cyber Security Centre (ACSC) Alert Service, to be informed of the latest threats and how to keep you, and your family, safe. Businesses, or larger organisations, may choose to partner with the ACSC to engage and draw upon collective understandings, experience, skills, and capabilities; so as to lift cyber resilience further within the community. The ACSC website provides information, tools, and a community that will help in your awareness of cybercrime.