SIMON CARABETTA *Project and Engagement Coordinator, WA AustCyber Innovation Hub*
LinkedIn/Website https://www.linkedin.com/in/simoncarabetta/

A communications and education professional turned cyber security advocate and influencer. Simon has led a number of projects focussed on raising the profile of cyber security in Western Australia and has helped provide support to small businesses as well as teams within the public and private sector. Simon continues to help grow WA's cyber security industry by educating high school students about careers and pathways in the sector.

TIP 1. ENABLE MULTIFACTOR AUTHENTICATION

Whether it's an account used for work, personal banking or social media, you must ensure that you've enabled multifactor (also known as 2 factor) authentication. This is a second layer of protection on top of a password – or passphrase, but more of that later – and will guarantee better security on your apps and devices. Multifactor authentication can be in the form of a one-time code sent to your phone/email or a biometric such as a finger print scan.

TIP 2. MOVE FROM PASSWORDS TO PASSPHRASES

When it comes to good password security, most people often assume that complexity in the password means that it's highly secure. This isn't exactly the case. Good password security is actually dependent on length, with a 16 character minimum being the standard. But how do you remember all those characters? Simple; just use a phrase – lyrics in a song, a movie quote, 4 random things on your desk right now – passwords are easy for people to remember but harder for cyber criminals to guess.

TIP 3. USE A PASSWORD MANAGER

Speaking of passphrases; you'll also need to use a different one for all of your different accounts. Banking, social media, email etc. these all require a separate and long passphrase in order to be secure. If you're thinking to yourself, "but how am I supposed to remember at least 12 different passphrases?" then the answer to that is a password manager. Using a highly secure decryption key, the password manager remembers all your passphrases, encrypts them, and unlocks them with one password. However, make sure that your password manager's password is secure, not forgotten, and also of a good length.

TIP 4. SIGN UP TO CYBER SECURITY ALERTS

Cyber attacks happen more frequently than people realise, with at least one occurring every 10 minutes to businesses in Australia. Fortunately, you can sign up to receive alerts on the latest threats and vulnerabilities as well as how to protect against them. The Australian Cyber Security Centre has an alert system that you can sign up to on www.cyber.gov.au. In addition to alerts, their website is also a wealth of information and resources to help you protect your business.

TIP 5. WHAT DO I DO IF I'VE BEEN ATTACKED?

There are many types of cyber attacks that can occur to small businesses, with the most common today being ransomware attacks. This is when the criminals encrypt data on your system, making it unavailable to you and your clients, only unlocking it once a ransom fee is paid. The Australian Cyber Security Centre works in tandem with all state and territory police departments to take cybercrime reports. You can call the following number 1300 292 371 or visit www.cyber.gov.au to report a specific type of cyber attack.

TIP 6.GET EDUCATED AND TRAIN YOUR STAFF

Cyber security awareness training is prevalent these days at most large corporations. However, small to medium sized businesses tend to miss out due to the cost of some providers or mistakenly thinking it's not important. There are a number of advisory and cyber awareness providers in Western Australia specifically to support small businesses. Making sure that you and your employees are aware of good cyber hygiene is vital to your ongoing business continuity and may be the difference between a devastating attack occurring or being thwarted.

TIP 7. 80-90% OF CYBER ATTACKS ARE HUMAN ERROR AND SOCIAL ENGINEERING

Unfortunately there is no 'silver bullet' for preventing cyber attacks. It's a complex issue that requires a multifaceted approach. While technical controls such as anti-virus and firewalls do a decent job, they're simply not enough. As in the previous tip, training your staff is key to preventing a multitude of attacks. Recognising the signs of suspicious emails and messages (known as phishing) is the first step, as phishing is usually the most common way in to your system for cyber criminals.

TIP 8. CYBER SECURITY STARTS AT HOME

Any unsafe online practices you're doing at home will almost certainly translate to the workplace. It's vital that you use good, safe cyber hygiene practices at all times. If there is a breach in your home network, then assume that your work accounts and apps have suffered a similar fate. With so much interconnectivity online and so much personal information available, knowing the safe online habits are really important to securing your work life and your personal life.

TIP 9. COMMUNICATE CYBER WITH YOUR SUPPLY CHAINS

Supply chain security is fast becoming a hot topic in cyber. No longer are cyber criminals carrying out attacks directly on large corporations, rather they are going through their supply chain businesses to find ways in. It's imperative that you discuss cyber security with your own suppliers and with those that you supply to. An attack on one business may spell disaster for many.

TIP 10. KNOW WHAT'S IN YOUR ECOSYSTEM AND UPDATE!

Ensure that you and the right people in your business are knowledgeable about the various apps, plugins and extensions that you are using. Some extensions that are installed may be out of date, no longer supported, or require updates in order to fix vulnerabilities. Ensure that you are constantly checking for updates and patching any security 'holes' as required. Whenever you're notified on your system about a large update, whether it be for your operating system, browser, or any apps in general, don't put it off. Update as required, as soon as you can.