PAUL HASKELL-DOWLAND *Associate Dean, Edith Cowan University*
LinkedIn: www.linkedin.com/in/pdowland/
Website: paul.haskell-dowland.com

Paul has appeared on local, national and international media commenting on current cyber issues with a global audience reach of more than one billion people. Paul has more than 20 years of experience in cyber security research and education in both the UK and Australia.

TIP 1. UPDATES, UPDATES, EVERYWHERE

We all know we should apply updates, so why do we not do it? Updates should be applied when available and checked regularly. Don't rely on automated patches - make sure they are being applied correctly and consistently.

TIP 2. PASSWORDS DON'T HAVE TO BE COMPLEX

Put simply: qwerty123 is bad; [4r4QnML9Hr>aHKM^WBj is better. But, while complex; lengthy, random passwords are more difficult to guess, they are impossible to remember (for the average human). Try combining a sequence of words as an alternative.

TIP 3. PASSWORDS SHOULD BE UNIQUE

Once you have a strong password, don't reuse it. Use a password manager to ensure that every password (particularly on websites) is unique. That way, if a password is compromised, it will only impact on that one site.

TIP 4. EDUCATION IS WORTH MORE THAN POLICY

You can establish policies and procedures for every conceivable eventuality… but encouraging cyber-safe behaviours in the workplace through training and education will pay dividends.

TIP 5. UTILISE MULTI-FACTOR AUTHENTICATION

Strong password selection is a good start, but you are still only a compromise away from being owned. Rather than depend exclusively on a single password, use multi-factor authentication where credentials are backed up by SMS, authenticator apps or tokens.

TIP 6. WHAT'S THE BACKUP FOR YOUR BACKUP?

Your organisation may have established backup procedures. But, have you tested them recently? Do you know how to restore your systems and data? Do you have backup copies stored off-site for resilience?

TIP 7. PUBLIC WI-FI CAN BE A BACKDOOR INTO YOUR SYSTEMS

While it may be very convenient to use free Wi-Fi outside of the office, is it secure? Most public Wi-Fi services are not inherently risky, but they are a public, shared facility. If you must use one, avoid accessing business systems or use a VPN to protect traffic from interception.

TIP 8. CHECK FOR SIGNS OF COMPROMISE

Monitor your accounts for misuse - especially bank accounts and credit cards. If you see anything suspicious, contact the provider. Regularly check email addresses and phone numbers on haveibeenpwned.com.

TIP 9. EVERY DEVICE IS A POTENTIAL THREAT

The plethora of devices in our daily lives opens complex avenues for compromise. Have clear rules on the use of network connected devices in the workplace. Don't forget automation technologies including air conditioning and lighting control systems.

TIP 10. DON'T FORGET FRIENDS AND FAMILY

Cyber security starts at home - if your employees demonstrate safe behaviours at home, they will bring them into the workplace. Encourage staff to explore cyber security concepts and to become champions for friends and family.