DR DAVID TUFFLEY - *Senior Lecturer in Cybersecurity at Griffith University*
https://www.linkedin.com/in/davidtuffley/

Dr. David Tuffley is a Senior Lecturer in Cybersecurity at Griffith University where he teaches cybersecurity governance, policy, ethics and law in the Master of Cybersecurity program. Before academia, David did consultancy in Australia and the United Kingdom to public and private sector clients.

TIP 1. EDUCATE YOUR DIRECTORS

Money flows down from the directors. It's essential that directors understand cybersecurity and can allocate the kind of funding needed for the latest prevention tools. If you are a director, be in no doubt that money spent on cybersecurity is a good investment. This is the best way to avoid catastrophic data breaches and damage to reputations.

TIP 2. COMPANY DIRECTORS NOW RESPONSIBLE FOR DATA BREACHES

Related to Tip 1. Amendments to the Security of Critical Infrastructure Act 2018 make company directors personally accountable for a cyber breach. On the 2nd December, 2021 the Security Legislation Amendment (Critical Infrastructure) Bill 2021 was passed and came into effect.

TIP 3. BE PROACTIVE, ANTICIPATE THE ATTACK

It is a certainty that your internet connected systems will be attacked. Not a matter of if, but when. Adopt a proactive mind-set and implement all possible countermeasures before the attack - and in all likelihood prevent the attack. Instil this proactive attitude in everyone from the top to bottom of your organisation.

TIP 4. ANTICIPATE THE SOCIAL ENGINEERING ATTACK (AKA PHISHING)

Most cyber-attacks succeed by tricking, scaring, and/or cajoling people into revealing their login details to third parties, usually via email/text; but also by phone call. Go to great lengths to educate everyone in how to recognise and avoid such attacks by not clicking on links in emails and text messages. Never, ever, give login details over the phone or by email.

TIP 5. KEEP SOFTWARE UP TO DATE

Keep software up-to-date, including browsers, anti-virus and other programs that have access to the internet. This can prevent attack methods that were current last month from succeeding today.

TIP 6. USE TWO FACTOR AUTHENTICATION (2FA)

Simple and effective, whether the code is generated by an authenticator app or sent to the person's smart-phone, there is no excuse these days to not be using 2FA.

TIP 7. USE STRONG PASSWORDS OR PASSPHRASES

12-14 characters is a good length with a mix of capitals, symbols and numbers. Better still: use a passphrase that can be longer. The phrase should be something personal, known only to you and be meaningful enough that you never forget it. End the phrase with a series of numbers that mean something important to you.

TIP 8. KEEP OFF-SITE BACKUPS THAT RUN AUTOMATICALLY EACH DAY

Ransomware attacks can cripple a business. Beat the crooks by installing automatic daily backups to the cloud. Or, if practical, also backup to an external hard drive that has an "air gap" when not in use. Then a ransomware crippled computer can be wiped clean, then OS and apps reinstalled with clean data restored.

TIP 9. LOCK COMPUTERS/SMARTPHONE ON IDLE

After a period of 15 minutes of inactivity, computers should lock and require a password or PIN to unlock. Smartphones default to a minute or less. Leaving an unlocked computer/phone unattended for even a short time is inherently risky unless you are in a secure environment.

TIP 10. CYBERSECURITY IS EVERYONE'S BUSINESS

Cultivate the mind-set in everyone in the organisation that cybersecurity is their responsibility. Social engineering attacks are the most successful attack vector. Regularly impress on people that an 'ounce of prevention is worth a pound of cure'. It can make all the difference.