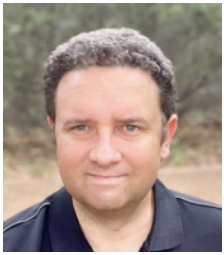

TYSON HORSEWELL *Freelance Consultant*
https://www.linkedin.com/in/horsewell/

A freelance IT consultant who has been working with small businesses for twenty years on IT related projects, Tyson has worked across a number of different fields from websites and IT support to security and networking.

TIP 1. KEEP YOUR SOFTWARE AND DEVICES UP TO DATE

Regularly update your operating systems, software, and applications to ensure that they have the latest security patches and updates, as these often address known vulnerabilities that cybercriminals can exploit. This is not only important for desktop computers, but also other devices such as tablets, phones, and smart devices also need to be kept up to date.

TIP 2. USE STRONG AND UNIQUE PASSWORDS

Avoid using easily guessable passwords. Instead, use complex passwords that include a mix of uppercase and lowercase letters, numbers, and special characters. NIST recommends a minimum of 8 characters and longer passwords are recommended. Also, use unique passwords for each account to prevent unauthorised access in case one account is compromised. Finally, use password managers such as LastPass or Nordpass to manage large numbers of passwords.

TIP 3. ENABLE TWO-FACTOR AUTHENTICATION (2FA)

Two-factor authentication adds an extra layer of security to your accounts by requiring a second form of verification, such as a text message or a fingerprint, in addition to your password. This can help prevent unauthorised access, even if your password is compromised. Make sure these are kept up to date when changing phones or numbers.

TIP 4. TRAIN YOUR EMPLOYEES

Educate employees about cybersecurity best practices, such as identifying phishing emails, avoiding clicking on suspicious links or downloading unknown attachments and being cautious with their personal and work-related information online. Generally, employees shouldn't be administrators on their computers and shouldn't be able to install software. It's worth checking out cyber.gov.au for more helpful information.

TIP 5. REGULARLY BACK UP YOUR DATA

Make sure to regularly back up your critical business data and store it securely offsite. This can help you recover your data in case of a cyber-attack or other data loss event - ideally, three backups in two formats. However, having a cloud and an off-site backup would be good enough for most.

TIP 6. USE FIREWALLS, CONTENT BLOCKERS AND ANTIVIRUS SOFTWARE

Install firewalls and antivirus software on all your computers and devices to protect against known threats. Keep them updated with the latest virus definitions. It is worth getting advice from a cybersecurity expert about your company's specific needs.

TIP 7. LIMIT ACCESS TO SENSITIVE INFORMATION

Only provide access to sensitive information and systems to employees who need it to perform their job duties. Implement strict access controls and regularly review and revoke access for employees who no longer need it. Refrain from having

generic accounts that allow multiple people to use the same account to access company data.

TIP 8. BE CAUTIOUS WITH EMAIL ATTACHMENTS AND LINKS

Be careful when opening email attachments or clicking on links, especially if they are from unknown sources or look suspicious. Verify the sender's authenticity and the email's content before taking any action. In Outlook and other email programs, turn off automatic remote content download; it's easier to spot fake emails and makes it harder for malicious senders to track activity.

TIP 9. REGULARLY MONITOR YOUR NETWORK

Set up security monitoring tools to detect and respond to potential cybersecurity threats in real time. Regularly review logs and other security data to identify any unusual activity that may indicate a security breach. Even a small office with a consumer internet connection could have a cybersecurity expert review their network setup periodically to ensure it's using the best possible practices.

TIP 10. HAVE AN INCIDENT RESPONSE PLAN

Develop a plan to respond to cybersecurity incidents, such as data breaches or ransomware attacks. This plan should outline the steps to take in case of a security breach, including how to notify affected parties, contain the damage, and restore normal operations. Having a cybersecurity consultant assist ensures that best practices are followed.