JAYA PRAKASH, *Director- Cybersecurity Practice, Borderless CS*
LinkedIn: www.linkedin.com/in/jayaprakashbcs
Company Link: https://www.linkedin.com/company/borderlesscs/
Website: https://borderlesscs.com.au

TIP 1. SECURITY AWARENESS AND TRAINING

Security awareness and training can inform you and your staff about good cybersecurity practices. Choose simple, focused, and concise training topics, and use periodic quizzes, contests, and rewards to keep employees interested and involved.

TIP 2. BUDGETING FOR CYBER SECURITY

Adequate cyber security controls are a crucial investment that should be included in your annual business plans and budgets. Don't install free software on your work computers; purchase licensed applications. Identify all business assets (such as computers and business information) and determine their importance and value to the business.

TIP 3. SECURE PORTABLE MEDIA

Portable media devices such as portable hard drives, USB flash drives, and secure digital (SD) cards are handy for transferring files between devices. However, due to their small size and portability, they are at a higher risk of getting lost or stolen, which could lead to a potential data breach.

TIP 4. PROTECTING BUSINESS INFORMATION ONLINE

To ensure the safety of your business, it is essential that they take necessary measures to safeguard business information while using the internet. Personal and business information comprises private or confidential details such as full names, driving license numbers, email and phone numbers, addresses, banking and other account information, and passwords.

TIP 5. BROWSING THE INTERNET SECURELY

Implement a site-rating tool as an extension to the browser on staff computers. This will help employees identify safe websites. Restricting the types of websites that employees are allowed to visit can help you exclude the sites that could compromise your business.

TIP 6. EMAIL SECURITY

Implement a spam filter - doing so will help you eliminate the most potentially harmful emails cybercriminals send. Don't click on unverified or suspicious links- even just clicking a link could give away sensitive information that a cybercriminal can use to hurt you and your business.

TIP 7. IMPLEMENT ACCESS CONTROL AND MULTI-FACTOR AUTHENTICATION.

Organisations should follow the principle of least privilege, where users have only the minimal functionality required to perform their tasks. Implementing access control and multi-factor authentication offers significantly more powerful security and protection against criminals.

TIP 8. DEVELOP AN INCIDENT RESPONSE PLAN

Organisations need a cyber security incident response plan as part of their disaster recovery and business continuity plans. Have emergency system boot DVDs or USB sticks prepared in case of a system crash. Properly label any sensitive information you have to ensure secure handling.

TIP 9. ENABLE SECURITY SOFTWARE

Organisations must implement secure configurations and enable anti-malware software on all devices to protect against known malware threats (e.g., viruses, worms, Trojan horses, ransomware, spyware….).

TIP 10. BACKUP AND ENCRYPT DATA

It is highly recommended that businesses regularly back up all their essential information in an external and secure location. Data backups play a crucial role in ensuring quick recovery from cyber security incidents like ransomware or malware and from natural disasters, equipment failures, or theft.