NAGESWAREE KODAI RAMSOONDER, *Cyber Security Presenter, Help Desk*

MY Business Incubator™ Western Australia.

LinkedIn: https://www.linkedin.com/in/nageswaree-kodai-ramsoonder-09b44b1b1/

Nageswaree has a master's degree in Cyber Security. She has been an author and presenter for international Conference on Computational Science and Computational Intelligence (CSCI'2020). She has been involved in the CyberCheckMe project at ECU as Content Developer. She is currently MY Business Incubator™ Cyber Security Presenter and Cyber Help Desk / Mentor and is passionate about boosting cyber security awareness.

TIP 1. CREATE UNIQUE PASSWORDS AND PASSPHRASES

A culture of poor password hygiene has been one of the major causes for data breaches as cybercriminals can easily crack weak passwords and gain unauthorised access. Unique, longer passwords and passphrases are recommended to lessen the various risks. Avoid using the same login credentials for different accounts.

TIP 2. USE ANTI-VIRUS SOFTWARE

An anti-virus software is crucial for detection and removal of malware, viruses and adware from your devices. Free online anti-virus software is not reliable, so ensure you buy only from a reputed and trusted software vendor. An IT services provider can install the anti-virus software on your computer devices at work to protect you and your employees. Make sure that your anti-virus software is always updated as new malware are emerging every day.

TIP 3. KEEP YOUR DEVICES UPDATED

Regular software updating is highly recommended as it not only upgrades the existing features but adds new features to the devices. Software updates also patches vulnerabilities in a computer system; thus, automatic updates should be enabled to prevent hackers from gaining access to your devices.

TIP 4. USE TWO-FACTOR OR MULTI-FACTOR AUTHENTICATION

Two-factor or multi-factor authentication should be turned on for both personal and work emails. Along with your password, you can opt to have a code generated and sent to you on your mobile device to verify your identity before allowing you to log in. It provides an extra layer of protection to all your accounts as it requires two or more different forms of identifications to grant you permission to log in.

TIP 5. BACKUP YOUR DATA ONLINE, OFFLINE AND OFF-SITE

Always conduct regular online, offline, and off-site backups, so that data can be restored in case of a ransomware attack, computer crash, natural calamities like fires and floods, or due to accidental property damage. It becomes vital to have an off-site physical backup which is more secure and helps to ensure minimum disruption of business continuity.

TIP 6. ALWAYS HOVER OVER LINKS AND ATTACHMENTS PRIOR TO CLICKING

Email scam/phishing has become the most common threat to businesses causing financial loss and damage to reputations. Ensure to always hover over the links and attachments before clicking to check where the URL are redirecting to, and to ensure that they are genuine links.

TIP 7. DO NOT USE UNKNOWN USB/FLASH DRIVES OR EXTERNAL HARD DRIVES ON YOUR DEVICES

Unknown or random removable media, USB/flash drives or external hard drives should not be used as they can infect your devices and even servers with malicious content and viruses. Cybercriminals can then steal, modify, and/or delete any information from your computer network, causing loss and leakage of data.

TIP 8. DO NOT LEAVE DEVICES UNATTENDED

Do not leave your devices unattended in plain sight and always log off or lock your computer with a password-protected screen saver before moving away from your computer. It can cause loss of privacy as intruders might read, change and/or erase sensitive and confidential information - putting the employer and the business at stake.

TIP 9. BE WARY OF WHAT INFORMATION YOU SHARE ON SOCIAL MEDIA

Be cautious about how much information you share about yourself on social media accounts and check your privacy control setting to verify which information can be made public or kept private. Avoid sharing critical personal information like your home address, date of birth or/and your daily routine schedule on Facebook, Instagram and/or Twitter as a cybercriminal can use your personal details and steal your identity.

TIP 10. AVOID MAKING FINANCIAL TRANSACTIONS USING PUBLIC WI-FI

Public Wi-Fi connection is not secure and using it for any transaction enables cybercriminals to intercept the data sent and received from your device. Cybercriminals can position themselves between you and the end point and install malware in your laptop/mobile device and can easily retrieve and access your banking details, accounts passwords and other sensitive information. Use your mobile phone's network instead and do not connect to any public Wi-Fi connection.