DR NOR MASRI SAHRI - *Senior Lecturer and Head of Cyber Security Research, Education and Network (CyberREN) University of Technology MARA Malaysia*
www.linkedin.com/in/normasri

TIP 1. PASSWORD MANAGEMENT

Password requirements are sometimes annoying, but please remember that this is one of the first lines of defence against cyber security attacks. Do not share your passwords with others even with your organisation's colleagues. By memorising the password created is the best way to avoid information leakage that could lead to further threats towards your organisation.

TIP 2. CYBER RISK ASSESSMENT

Identify thoroughly what is valuable to your organisation, particularly in terms of information. Determine what assets you have in place to process, store, transport, and safeguard your sensitive data; as well as how securely they are configured. Identify what are the possible scenarios in which your asset (particularly sensitive information) could be compromised?

TIP 3. INVEST IN CYBER SECURITY

Investing in cyber security is no longer an option. It's a requirement. The best way to avoid attacks and preserve your digital assets is to take a proactive approach to cyber security. Fun fact - SMEs are seen as easy targets by many cyber thieves, and they are more inclined to target them when launching an assault.

TIP 4. THINKING LIKE YOUR ENEMY

Examining your company through the eyes of possible attackers in order to discover what is most valuable. Determine your requirements so you can identify your crown jewels - and what is most important in terms of security.

TIP 5. LOCAL GOVERNMENT INITIATIVES

Most local governments around the world offer help and advice for SMEs to make sure they are prepared for any cyber security risk. Rather than waiting to be helped, get to know which government agencies in your place offers to provide the help.

TIP 6. EDUCATE ALL MEMBERS OF THE ORGANISATION

From top to bottom of your organisation, no one is excluded to equip themselves with the fundamentals of cyber security. To have regular sessions on understanding the principle of cyber security is an example of a good practice for the organisation.

TIP 7. AWARENESS

The key to a successful security awareness program is ensuring that the appropriate training is given to the appropriate personnel. All users are vulnerable to cyber dangers; however, certain employees are more vulnerable than others. Focus on high-profile groups.

TIP 8. PLANNING TO USE - OR CURRENTLY USING - WEB APPLICATION?

If you plan, or currently use, web application for your businesses; choosing to use Secure Socket Layer (SSL) for your web application reduces the threat of cyber threats dramatically to ensure the safety of any information transferred in and out of your organisation. Never heard of SSL? Well, most organisations use web browser in their everyday work. Noticed the "lock" figure at the web address section?

TIP 9 CYBER HYGIENE?

Cyber Hygiene is about teaching oneself effective cyber security behaviours so that you can keep ahead of cyber dangers and internet security problems. Cybercriminals will be less likely to cause security breaches or steal personal information if you establish a practice around cyber hygiene - such as using antivirus software that can be used to search for viruses, regularly change passwords, keep software and operating systems up to date and wipe your hard drive.

TIP 10. RESILIENCY: BACKUP AND PROTECTION

We need to backup data since the primary data failures can be caused by hardware or software failures, data corruption, or a human-initiated event like a hostile attack (virus or malware) or data deletion. It's a copy or archive of vital data kept on your devices, such as a computer, phone, or tablet, and it's used to restore that original data in the event of a data loss.