SHAVEEN WEERASEKERA *Cyber Security Engineer , Motherwell Automation*
LinkedIn/Website Shaveen Weerasekera | LinkedIn

Shaveen is passionate about cyber security and penetration testing. He is a cyber security engineer with experience in penetration testing, software engineering and system administration. Currently, he is actively involved in systems automation and OT security.

TIP 1.CYBER SECURITY AWARENESS

Being aware of the potential risks of daily online activities is a responsibility of anyone who is interacting with cyberspace. Cyber security awareness, therefore, involves keeping users up to date with both the advantages and disadvantages of engaging in online activities, the dos and don'ts when faced with a cyber security threat, and the precautions that can be taken to avoid experiencing cyber attacks such as phishing, ransom ware and password attacks.

TIP 2. BE SCEPTICAL: YOU DON'T HAVE TO OPEN EVERY EMAIL

Is this email work related? Should I click on this link? Am I expecting this email or call? Be sceptical. We receive hundreds of emails a day and a portion of that is spam, or pretending to be someone else. Emails related to marketing, promotions etc. can be ignored without opening. Always ask yourself those questions before you open external emails.

TIP 3. INVEST IN CYBER SECURITY

Cyber security sounds expensive. But, in the long run it will save your company financially by preventing potential cyber-attacks. Cyber-attacks may lead to serious financial, reputational damages, downtimes and possible lawsuits. Be proactive. Invest in cyber security.

TIP 4. MFA

Multi Factor Authentication (MFA) is a security measure where the user must provide two or more proofs of identity to an authentication mechanism in order to be granted access. Cyber criminals may gain access to your password, however, your account will not be compromised until they provide the other proof of identity.

TIP 5. PASSWORD MANAGEMENT

Password attacks are one of the most commonly occurring cyber attacks of all time. Always use complex passwords and avoid re-suing passwords. Remembering different passwords can be a difficult task. You can overcome this trouble by using a password manager to store passwords securely and locally. Again, remember to use a strong master password for the password manager.

TIP 6. REGULAR BACKUPS

Loss of data will always be a sad tale. Data losses occur due to various reasons, such as hardware failure, theft, natural disasters, accidental deletes, and ransom ware attacks, etc. Data losses can result in significant financial damages to an organisation. However, this can be easily overcome by performing regular backups. Backups will ensure minimum downtime and quick recovery from data loss incidents.

TIP 7. USE ENCRYPTION

The email you send, and the file you share, could go around the world before it reaches its destination. Encryption is a method of encoding data. This method converts the original data to an unreadable form which can only be decoded by authorised people. Encryption can be used as another layer of security when data is transferred via the internet.

TIP 8. ANTIVIRUS

Malware is malicious software designed to harm your computer, steal or delete data, or use your resources for other purposes. Malware can spread through emails, attachments, USBs and malicious websites. Modern antivirus programs detect and take action against malware that are causing harm to your computers and update automatically on a regular basis.

TIP 9. HIDE BEHIND A FIREWALL

You might already have many security practices in place. But if you're using the internet, it is recommended to have a firewall placed, securing your network. Without a firewall you're open on the internet, accepting every connection. A firewall blocks unsolicited network traffic, blocks traffic going out to malicious sites and gives you more control over the network.

TIP 10. NETWORK SEGMENTATION

Network segmentation helps reduce internal and external threats. Separating users/departments improves security and privacy by ensuring user access is limited to their respective network segments. Furthermore, this simplifies network and user management. Enforcing and controlling policies can be done at a group level.