SANJAY SHARMA, *Security Analyst, DXC TECHNOLOGIES*
www.linkedin.com/in/sanjay-sharma-663669126/

Sanjay currently works at DXC Technologies as Security Analyst. He has developed a broad understanding of cyber risk management and mitigation strategies. With a solid background in security management frameworks, he has experience working with different technologies and SOC tools. He previously worked as Senior ICT Support officer with the Department of Health, WA. He has won the 'Research and Innovation – Postgraduate Student Project of the Year" INCITE AWARDS in July 2021.

TIP 1. BE ALERT

Social Engineering attempts are one of the biggest threats to your business's health. A single phishing attempt can result in huge loss. Phishing emails even look legitimate as they are coming from the legitimate or trusted vendors such as Microsoft, banking, or your internet providers. These emails include attachments, or sometimes ask you for Personal Identifiable Information (PII). So, always scan for email attachments and take a moment while responding to such emails. Your proactive response can prevent many cyber attacks.

TIP 2. CYBER AWARENESS IS IMPORTANT

Cyber awareness is no longer an option, it is a major requirement of today's business. Cyber awareness training is the first step of defence against the cyber-attack tactics, or malicious attempts. In organisations, cyber-hygiene practices should be a shared responsibility for all the system users, and there should be regular training to educate organisation's workforce about today's cyber threats and mitigation strategies. Continuous evaluation of these cyber-attacks could significantly reduce the risk of being targeted.

TIP 3. USER ACCESS CONTROL

Organisations need to examine people, process, and technology to identify weak points. Physical and logical access control policies can help organisations to reduce the risk of unauthorised access. There is no need of providing admin privileges to every user, restricting access to system users ensures the security of your organisation from bad actors.

TIP 4. STRONG AND COMPLEX PASSWORDS

Always use a lengthy password with a combination of numbers, special characters , upper- and lower-case letters. Password Manager is one of the best options for generating strong and complex passwords. Password management software uses 256-bit AES military standard encryption, and it is still impossible to break.

TIP 5. REGULAR CYBER RISK ASSESSMENTS

It is important that organisations should carry out cyber-security risk assessments regularly. Without having cyber-risk assessments there is limited impact of cyber-defence procedures. Step-by-step cyber security frameworks will help your business to prevent security incidents.

TIP 6. BACKUPS

Backup is the copy of all your important information. You need to setup automatic backups to ensure you have a complete copy of your data. Once you have online backups in your system or cloud storage - make sure to create offline backup and this offline backup should not be connected to the internet and stored securely. These backups help to restore all the information in case of data loss or a ransomware attack.

TIP 7. REGULAR PATCH MANAGEMENT

Cyber-attackers always target known vulnerabilities in OS or third-party applications. Organisations need to keep all the devices and software's up to date, i.e., properly patched. Patch management is important because an attacker can exploit the vulnerability if not patched on time. Patch management policies helps the organisation to set clear rules for the patching process and avoid exposure to cyber-attacks.

TIP 8. CONTROL ACCESS TO YOUR NETWORK

Network Access Control (NAC) keeps the unauthorised users out of your private network and non-compliant devices only have restricted access to business resources.

TIP 9. MULTIPLE LAYERS OF SECURITY

Organisations need to adapt a layered security approach effectively. Multiple security controls are crucial to protect the system users, business networks and sensitive information. Layered security approach involves the three controls:- admin, physical and technical controls. These defence in depth strategies provides defensive redundancy, i.e., if one of the security layers fails/down other layers keep the data safe.

TIP 10. RISKS OF USING PUBLIC WI-FI

The first question comes in mind while using public Wi-Fi is "SECURITY", because public Wi-Fi comes with various risks that you need to aware of. Try not to use public Wi-Fi for banking transactions, accessing business systems or sensitive data.