MARLON I. TAYAG, *Dean, School of Computing - HAU*
Website www.marlontayag.net

Dr. Marlon Tayag, DIT, is the Dean of the School of Computing at Holy Angel University, with over 18 years of experience in IT. He specialises in IoT security, blockchain distributed app development, ethical hacking, and forensics. A certified expert in Cisco, Microsoft, and CompTIA technologies, Dr. Tayag has taught mobile application development and information security at the graduate level at SPCF. He has also lectured at The Future University in Sudan. Currently, he teaches cybersecurity and Cisco-related subjects as a guest lecturer at HAU's Graduate School. Holds numerous certifications, including Cisco, Microsoft, CompTIA, and Certified Ethical Hacker, and has taught globally, including at The Future University in Sudan.

TIP 1. CHANGE PASSWORD REGULARLY

Password change should be a culture to everyone. Put in place a policy to change passwords at regular intervals (monthly). As an additional measure, small businesses should enable multi-factor authentication (MFA) on employees' devices and apps.

TIP 2. LOCK PC POLICY

Don't leave your computer alone. Even at work, someone might try to look at your files. To keep your information safe, set your computer to lock itself after 30 seconds of not being used. This way, no one can see what you're doing when you step away.

TIP 3. DEPLOY ANTIVIRUS SOFTWARE

Choose a program that blocks viruses, malware, and phishing attacks. It should also have tools to clean infections and restore your device to its original state. Remember to keep your software updated for ongoing protection against new threats.

TIP 4. USE PASSWORD MANAGERS

Safeguard your business by using a password manager. It creates strong, unique passwords for all online accounts, protecting sensitive data and preventing data breaches, ultimately building customer trust. This is also a tip to help staff not to reuse the passwords. It's also safe to note that you need a secure password manager.

TIP 5. RESTRICTING ACCESS TO WI-FI NETWORKS

If your business has Wi-Fi available for employee use, make sure it is secure (password-protected) and is hidden. If you provide public Wi-Fi for customers, ensure it only allows users internet access, not business critical network access. Never use public Wi-Fi hotspots to access your company network, as data can often be transmitted in plain text for potential Wi-Fi detectors to see.

TIP 6. USE OF TRUSTED TECHNOLOGIES

It is essential to install only trusted technologies (both hardware and software) to prevent cyber-attacks. Discourage staff from downloading third-party apps, or apps from unknown sources, as they may contain or spread malware on the network.

TIP 7. STAY INFORMED ON THE LATEST CYBER NEWS

Cybercriminals are always getting smarter. To protect your business, you need to stay informed. Read about cybersecurity safe tips, attend online talks, and join industry groups. Knowing what to expect can help you stay safe.

TIP 8. LIMIT ACCESS TO SENSITIVE DATA

Within your business, restrict the number of people with access to critical data to a minimum. This will minimise the impact of a data breach and reduce the possibility of bad faith actors from within the company gaining unauthorised access to data. Set out a plan which outlines which individuals have access to certain levels of information, so that roles and accountability are clear to all involved.

TIP 9. MOBILE DEVICE SECURITY

Your employees' smartphones are potential gateways for cyberattacks. Equip them with robust mobile security software. Look for antivirus protection that guards against viruses, malware, and phishing. Ensure the software can clean infections and restore devices to their original state. Regular updates are crucial to staying ahead of emerging threats. This layered defence protects your business data and maintains customer trust.

TIP 10. BACKUP DATA DAILY EXTERNALLY

To help, make use of a backup program that automatically copies your files to storage. In the event of an attack, you can restore all your files from your backups. Choose a program that gives you the ability to schedule, or automate, the backup process, so you don't have to remember to do it. Store copies of backups offline so they don't become encrypted or inaccessible if your system suffers a ransomware attack.