SAMUEL NG, *Director, Cybersecurity & Analytics, Hong Kong Applied Science and Technology Research Institute (ASTRI)*
LinkedIn/Website: www.linkedin.com/in/samuel-n-986751116

Passion fuelled cybersecurity professional with leadership trained by armed forces, Samuel has extensive experience in all cybersecurity domains from both technical and management perspectives. He brought value to organisations by balancing governance, controls, and business strategies ultimately upholding the CIA Triad (Confidentiality, Integrity, Availability) at highest standards. As a 14-years Malaysian army veteran with a Master's Degree and multiple infosec-recognised certifications, he progressed his career to Hong Kong, contributed to various sectors including: banking, telecommunication, cloud, IT infrastructures, start-ups etc. Currently exercising his expertise in Hong Kong Applied Science and Technology Research Institute, responsible for strategic planning and leading research directions of cybersecurity and data analytics.

TIP 1. BE IT BIG OR SMALL, YOU ARE ALWAYS A TARGET

The mindset of "I am too small to be attacked" is the fundamental reason why some businesses fell victim to cyber-attacks; leading to bigger losses which heavily impact the operations and revenue of a business. Threat actors continuously expand their "territory of compromise", either to obtain valuable information, piggybacking on victim's infrastructure or both. Risk-based approach would be helpful for understanding the exposure and mitigate accordingly balancing cost, effort and risks.

TIP 2. TOO GOOD TO BE TRUE? LOOK AGAIN

Having this sense will keep you away from trouble and save your organisation a hefty sum of cyber-attack incident, which cost millions of dollars annually. When you are not paying for a product, you are the product! Threat actors lure victims with a sense of urgency, greed and fear of losing in order to further their exploitation through phishing and other tactics.

TIP 3. GUILTY UNTIL PROVEN INNOCENT

Always check and validate the source when you encounter something. Be it an email, message, or a person's request. Only proceed when validation is obtained and report to the proper channel or authorities when something, or someone, sounds or acts suspiciously.

TIP 4. STRIKE A BALANCE FOR YOUR PASSWORDS AND CONVENIENCE

It's painful to have different passwords for all your online accounts. While it can keep you safe, having a balance for security and convenience is a long-term strategy for cyber resiliencies, both personal and organisational. To create a password: be creative, long and complicated, but make it personal and easy for yourself to remember so - when one of your accounts are compromised, you will be rest-assured that others are still safe.

TIP 5. MULTI-FACTOR AUTHENTICATION

Many platforms now offer the convenience of this additional protection layer. MFA requires minimal amounts of effort, but largely improves security by verifying it's you who are accessing the accounts, not someone unauthorised.

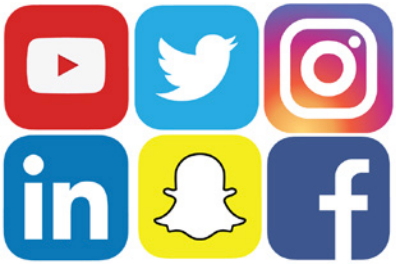
TIP 6. RADIO SILENT AFTER YOU ARE DONE

Mobile devices (with both your personal and company data) can be hacked wirelessly without the owner's interaction, practically even when your phone is in your pocket. Turn off all wireless features such as Wi-Fi, Bluetooth, AirDrop, etc when not in use

TIP 7. AVOID HAVING 'ALL EGGS IN ONE BASKET'

A proper risk assessment will identify the location, criticality and sensitivity of all your company data. A clear view of risks associated with multiple location of data is stored, combined with appropriate security controls based on the level of data criticality, will not only improve security, but keep you out from regulation and compliances issues as well

TIP 8. DON'T LIVE IN SOCIAL MEDIA



Without due care, sharing too much information on social media (such as: name, phone numbers, corporate email addresses and personal locations) can be used by threat actors not only in identifying theft, but information to fuel their bigger attacks such as: phishing, external and internal exploitations, password guessing with partially known information, etc…….

TIP 9. FOLLOW THE RULES – COMPLIANCE TO REGULATIONS

Adhering to local regulations and incorporating globally recognised cybersecurity standards not only helps your organisation to avoid fines and penalties; but also protects and improves your business reputation by building trust between your customers, partners, stakeholders and regulators

TIP 10. FUTURE PROOF YOUR CYBER DEFENCE, BECAUSE THREAT ACTORS DO TOO

Cyber-Defence with Artificial Intelligence and Machine Learning will be a powerful tool in the looming future. Threat alert fatigue and human errors are obvious pain points in cyber defences. Attackers are rapidly moving into Artificial Intelligence and emerging technologies (such as cloud computing) to enhance their offensive tactics, why shouldn't the defenders?