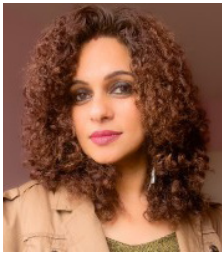

DR. SHEEBA ARMOOGUM - *Senior Lecturer, University of Mauritius*
LinkedIn: https://www.linkedin.com/in/sheeba-armoogum-phd-cybersecurity/
Website: https://sites.google.com/uom.ac.mu/sheebaarmoogum/

Dr. Sheeba Armoogum has over 16 years experience in teaching and research. Her field of research includes cyber security, cyber forensics and cyber psychology. She holds a PhD in cyber security and has a patent in the cyber security field. She served as a speaker for several discussion panels and events. She is certified in Research Ethics and Evaluation. She is also a cyber security subject specialist at national and international level.

TIP 1. FOLLOW CYBER HYGIENE FOR A SAFE CYBERSPACE BROWSING

The journey on cyberspace has become intensely complex with the escalating advancement in technology. It is vital to inculcate cyber hygiene as part of our daily routine to resist cyber threats and online security issues. Cyber hygiene is a set of routine practices for ensuring the safe management of critical data of organisations and also to prevent cyber criminals from data breaching.

TIP 2. USE THE RIGHT TOOL TO PROTECT YOUR DATA

With an availability of enormous tools for securing data on the computer and network, it is dilemmatic for decision-making on the right tool of choice. It is essential to encompass the organisation computer systems with basic security software like antivirus, anti-malware, antispyware and network firewall with regular updates and routine checkups.

TIP 3. MOVE FROM SYSTEM-CENTRIC TO SYSTEM AND PEOPLE- CENTRIC

Businesses focus mainly on the organisation's data, systems and networks. Although employees are one of the assets in any organisation, they can be the biggest threat for a security breech. Moving from system-centric business perspective to system and people-centric work perspective can minimise job switching. Job switching is one of the root causes for a security breech. The confidential data and information acquired by the employees during their stay can be compromised once they leave the organisation.

TIP 4. CREATE INDIVIDUAL ORGANISATION SECURITY FRAMEWORK

Hackers and Intruders can invade any network by learning the usage pattern of the on-shelf security software. A cyber security research development unit for an organisation can devise custom made off-shelf security software to enhance the security layer of the on-shelf security software and camouflage the network from a security breech.

TIP 5. ESCALATE THE ROLE OF CYBER PSYCHOLOGY TO ENHANCE CYBER SECURITY

Cyber psychology focuses on the psychological behaviours of cyber users to identify certain psychological phenomena which emerge as a result of the user interaction with the cyberspace. The aftermath of this impact will affect the offline life of an employee. It is necessary to escalate the significance of employee behaviour to mitigate the victimisation of cyber attacks - like social engineering, cyber bullying and online privacy invading due to psychological manipulation.

TIP 6. ADOPT A CYBER SECURITY RISK MANAGEMENT WORK CULTURE

The heightened cyber security risks have become difficult to administer due to the complexity of the risk and the unknown approaches by the hackers. For the continuity of the business, it is mandatory for any organisation to pursue a culture to practice a routine inspection of known cyber security and mysterious risks.

TIP 7. SEPARATE PERSONAL DEVICES FROM WORK DEVICES

Mobile devices have facilitated people to accomplish their work ubiquitously. This work culture encompasses the security threats where data and information become vulnerable. It is worthwhile to separate personal devices from work devices to secure both personal and organisational data.

TIP 8. CONCEAL YOURSELF FROM CAMERA VULNERABILITY

Build-In cameras and wireless webcams are vulnerable to cyber threats. If your device has been compromised due to a virus or malware, cybercriminals could then easily turn the camera on or off as well as disable the LED light to avoid detection. It is recommended to cover the camera of your device if not in use.

TIP 9. TRANSIT FROM CYBER THREAT PREVENTION TO CYBER RESILIENCE

It is time for organisations to transit from mere cyber threat prevention methods to cyber resilience by focusing on the ability to respond to cyber attacks, mitigating possible threats while protecting critical data and resume business operations.

TIP 10. REINFORCE CYBER SECURITY AWARENESS PROGRAM ROUTINELY

Reinforce employee's cyber security knowledge by performing routine cyber security awareness training. Eventually it will help the employees to understand the potential risks and threats associated with the organisation systems, networks and devices. It is necessary to make the employees aware on the organisational security policies to avoid them becoming a victim of cyber attacks.