KERRY-LYNN THOMSON *Professor of IT, Nelson Mandela University, South Africa*
https://ebet.mandela.ac.za/About-the-EBET-Faculty/Meet-our-Professors/Prof-Kerry-Lynn-Thomson

Kerry-Lynn has over 15 years of experience in information and cyber security research and education in South Africa. She chairs the IFIP Technical Committee 11 Working Group 12 (Humans Aspects of Information Security and Assurance), has published over 40 papers in journals and conferences, and her research interests include cyber security awareness and education, with a focus on the human aspects of cyber security.

TIP 1. INVEST TO PROTECT

Make sure to invest in the security of your organisation through a comprehensive and layered cyber security strategy, and the supporting technologies, to protect critical organisational assets. This layered security, also known as defense-in-depth, allows for security to be implemented in overlapping layers for the prevention, detection and response to attacks. Security layers could include antivirus software, firewalls, authentication, email spam filters and intrusion prevention systems.

TIP 2. ENFORCEMENT IS KEY

Establishing clear information and cyber security policies, and related procedures, is imperative. However, policies without enforcement are merely empty promises. Without proper communication and enforcement, even the strongest security policies may not protect your organisation.

TIP 3. EMPLOYEES CAN BE THE STRONGEST LINK

The majority of security breaches can be attributed to humans and human error, and employees are often seen as the weakest link in cyber security. However, with a focus on employee cyber security awareness and training, based on established security policies; employees could become the strongest link in the protection of your organisation. Employees must be empowered to know why cyber security is important and how they can protect their organisation from cyber threats.

TIP 4. GO PHISHING

One mistake by one employee clicking on the wrong link and being 'caught' in a phishing attack could lead to devastating consequences for your organisation. Phishing simulation training can assist your employees in avoiding and reporting potential cyber threats that could compromise an organisation, including ransomware, phishing and malware. Phishing simulations can further help employees understand the dangers of social engineering.

TIP 5. CREATE A PATCH MANAGEMENT CYCLE

Patch management is essential in distributing and applying updates for operating systems, applications, and network devices. These updates are necessary to patch vulnerabilities, errors or 'bugs' in the software which may otherwise leave your organisation open to exploitation. A strategic approach for updating and patching software should be used as part of a patch management cycle that is security-focused and prioritised.

TIP 6. FREE WI-FI MAY BE COSTLY

Employees travelling for business, or simply working from a coffee shop, may connect to free, public Wi-Fi to perform various tasks. Doing this without taking proper security precautions, however, exposes them to a variety of cyber threats, including man-in-the-middle attacks, session hijacking, loss of confidential information and eavesdropping. Virtual Private Networks (VPNs), together with multi-factor authentication, are recommended when using public Wi-Fi and should be enforced through your organisation's security policies.

TIP 7. PUT THE RIGHT FOOT(PRINT) FORWARD

Cyber criminals may be able to target the employees of your organisation through their digital footprint, which is created both actively and passively when they are online. Consequently, employees should not disclose business-related information online or through social media. Ensure that your security policies have clear guidance for employees posting on social media, as over sharing is often an enabler for social engineering.

TIP 8. DON'T FORGET ABOUT MOBILE DEVICES

Many of your employees may be using their personal mobile devices for work purposes, which can blur the line between convenience for employees and introducing risk into your organisation. Clear policies should be created about mobiles device use for work, and it must be ensured that your employees understand that their mobile devices could be potential attack vectors.

TIP 9. MULTI-FACTOR AUTHENTICATION

Make sure employees are who they say they are by using multi-factor authentication, where employees need to provide at least two pieces of 'evidence' when authenticating. This 'evidence', or factors, can be something they are, something they know or something they have. The chances of multiple factors being compromised is fairly low, so asking for multiple authentication factors provides a higher level of assurance of an employee's identity.

TIP 10. EXPECT THE UNEXPECTED

Your organisation should have a coordinated incident response plan that specifies the procedures that should be followed when a cyber-attack occurs. This incident response plan should include the procedures for all employees to follow if a cyber-attack is suspected or occurs, and the main goals are to minimise impact and for rapid recovery.