DR NICKSON M. KARIE - *Cybersecurity Research Fellow, Cyber Security Cooperative Research Centre, Edith Cowan University, Perth, Australia.*
LinkedIn: https://au.linkedin.com/in/dr-nickson-m-karie-a247a620

Nickson M. Karie received his PhD degree in computer science from the University of Pretoria, South Africa, in 2016. Currently, Nickson is a Cybersecurity CRC Research Fellow at Edith Cowan University, Security Research Institute, Perth, Western Australia. He has more than 10 years experience in academic research, teaching, and consultancy in different countries including India, Kenya, South Africa, Swaziland, and Australia. His research interests include intrusion detection and prevention, information and computer security architecture, network security and forensics, mobile forensics, and IoT security. He is also actively engaged as a high impact international conference and journal author and reviewer.

TIP 1. ALWAYS PROTECT SMARTPHONES AND OTHER MOBILE DEVICES

With the emergence of 'Internet of Things' (IoT) technologies, any device can connect to another. This has made individual and business smartphones and devices a potential target by hackers using over a million known types of mobile malware. Businesses and individuals can protect their devices by patching them, using difficult passcodes, and by only installing applications from trusted sources.

TIP 2. ALWAYS REMEMBER YOU ARE A TARGET TO HACKERS

Small businesses, as well as individuals, should not make a fool of themselves thinking "It will never happen to me". As long as you own a digital device, either at home or at work, that can connect to another digital device, you are at risk - and the chances that you can be hacked are always high. Businesses and individuals can keep safe by never exposing personal and financial information to anyone.

TIP 3. NEVER USE PUBLIC WI-FI FOR OFFICIAL WORK

Unless you are using a strong and trusted Virtual Private Network (VPN), never use public Wi-Fi services if security is a priority to you, especially Wi-Fi offered free of charge. Using a VPN will ensure that the traffic between your device and the VPN server is always encrypted; thus making it hard for criminals to access any individual or business data on your device.

TIP 4. ALWAYS THINK BEFORE YOU ACT OR CLICK ONLINE

Even though businesses and individuals have the freedom to do whatever they want online, it does not mean one should ever be reckless. With malware and sophisticated phishing techniques becoming the norm, businesses and individuals must safeguard their online accounts and all information on them. Always use unique and strong passwords. Never reuse passwords at any time. Never click or respond to requests you are not fully aware of; especially through emails, text messages, phone calls, and web pages.

TIP 5. ENSURE GOOD PATCH MANAGEMENT

Patches are not optional when it comes to correcting errors, vulnerabilities or bugs in an existing business or individual software. Businesses can stay safe by ensuring that all operating systems, applications, and embedded systems in use are up to date. A good patch management process ensures that all business and individual IT assets are not susceptible to exploitation. Patching is also good for supporting business system uptime and compliance.

TIP 6. GOOD PASSWORD MANAGEMENT IS NOT OPTIONAL

Always store and manage passwords efficiently as it's a good way to prevent unauthorised access to existing IT assets. With the many passwords that a business or individual can have, it can be tempting to take shortcuts or reuse the same passwords for different accounts. Consider a password manager to help in maintaining strong and unique passwords for all existing accounts.

TIP 7. CONSIDER USING TWO OR MULTI-FACTOR AUTHENTICATION

Businesses, and individuals, can enhance their security by using two or multi-factor authentication as this adds a security layer on top of the existing traditional username and password before being granted access to a website or application. With multi-factor authentication, it is very hard for hackers to be granted access to data by just stealing one of the authentication factors and also very hard for hackers to steal a complete set of credentials necessary to facilitate successful logins.

TIP 8. NO SOFTWARE IS IMMUNE

It is a known fact that "No connected machine is totally immune". This principle applies to software as well. Businesses and individuals should know that "No software is totally immune". With the advancements in technology, even trusted software in the market, is becoming a target for viruses. Always have an extra layer of security to protect business and individual data against cyber attacks.

TIP 9. USE A VIRTUAL PRIVATE NETWORK (VPN) WHEN WORKING FROM HOME

A growing number of employees are currently working from home as a result of the COVID-19 pandemic. Cybercriminals have, in recent times, targeted employees working from home to steal business or individual data. It is therefore important that employees working from home use VPN to connect to workplace networks, as well as secure their web browsing and remote network access.

TIP 10. ALWAYS AND FOREVER BACK UP YOUR DATA

Storage technology is becoming cheaper, making it easy for anyone to back up their data every day. Both physical onsite, as well as cloud or remote storage facilities, are now available to anyone. In the case of ransomware or malware attacks, data backups can help business organisations recover very quickly by restoring their systems with a recently performed backup; thus ensuring zero impact on performance.

"The work has been supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme."