**DANIEL MAKUPI** *Lecturer, Zetech Univeristy*
LinkedIn/Website www.linkedin.com/in/dr-daniel-makupi-68552680

Makupi is an accomplished professional in the field of IT security and audit, holding a PhD in the same discipline. With extensive expertise in cybersecurity, Dr. Makupi is recognised for his contributions to enhancing digital security frameworks. His academic background and practical experience equip him with a deep understanding of security protocols, risk management strategies, and auditing practices. Driven by a passion for safeguarding digital environments, he continues to contribute significantly to the advancement and resilience of IT security systems.

## TIP 1. CONTROL VISIBILITY ON SOCIAL MEDIA SITE

Periodically, social media sites update aspects of settings and options. Subsequently ensure you should also update your privacy settings. Make sure you also restrict who can see your posts, tags and who can troll to your profile details. In addition, a good practice is ensuring you can limit audiences of your past posts. This in a long way reduces the risk of unauthorised access or identity theft.

## TIP 2. CONTINUOUSLY MONITOR AND AUDIT CONNECTED DEVICES

Proliferation of connected devices is a major issue across different jurisdictions worldwide today. Periodically review your network connections to help you gain control of your devices. At any given time, if you realise an unfamiliar device, it's always a good practice to ensure they are not from unauthorised end points targeting towards compromising your network.

## TIP 3. USE MULTI-FACTOR AUTHENTICATION (MFA) FOR FINANCIAL SYSTEMS

Controlling access to financial platforms is a challenge, considering the monetary value of the systems. The security measures of member access to accounts and services on online financial platforms can be assured through MFA. It guarantees two or more verification factors to access the system, by adding an extra layer of security beyond the conventional username and password.

## TIP 4. SEGMENT YOUR ORGANISATIONAL NETWORK

Consider segmentation of your network between your own organisational devices and employees or external devices that may be from a 'bring your own device' environment (BYOD). At each segment, ensure authentication, access controls, and endpoint security measures. For each of the segments:- independently consider regular audits so as to guarantee security and minimise distributed lapse.

## TIP 5. USE OFFICIAL APPS FOR MOBILE MONEY TRANSACTIONS

Mobile money has attracted voluminous transactions lately with the proliferation of smartphones. Consider using official apps from trusted sources, and keeping your device and apps updated with the latest security patches. This approach will ensure unauthorised access, reducing fraud and protecting your funds. Including avoiding use of public Wi-Fi networks for transactions; rather use mobile data or a VPN (Virtual Private Network) for added security.

## TIP 6. BE AWARE OF PHISHING SCAMS

Request of personal information or prompt through clicks either through emails, messages, or websites without proper verifications should be avoided. The authenticity of the source should be identified for legitimacy. The majority of the fraud on personal data is divulged when an individual is tricked into shareing sensitive information.

### TIP 7. REGULARLY UPDATE YOUR SOFTWARE AND DEVICES

Keeping your operating systems, applications, and devices up to date is crucial for cybersecurity. Software updates often include patches for security vulnerabilities that hackers could exploit. By staying current with updates, you reduce the risk of falling victim to known security flaws. Make it a habit to enable automatic updates wherever possible, and regularly check for updates on devices that don't update automatically. This simple step can significantly enhance your cybersecurity posture.

### TIP 8. IMPLEMENT CONTINUOUS MONITORING AND INTRUSION DETECTION

Due to their constant connectivity and interaction with personal data, wearable IoT devices can be attractive targets for cybercriminals. Implementing continuous monitoring and intrusion detection systems helps in promptly identifying and responding to any suspicious activity or potential security breaches. This proactive approach allows you to detect anomalies, unauthorised access attempts, or unusual data transmissions early on, minimising the impact of potential cyber threats. Additionally, consider using security solutions that provide real-time alerts and notifications, enabling timely action to mitigate risks and protect the privacy and security of wearable IoT device users.

### TIP 9. RECONNAISSANCE AND INFORMATION GATHERING IS KEY WHEN CONDUCTING PENETRATION TESTING

Use both passive and active techniques to gather intelligence about the target environment, identify vulnerabilities, and understand network topology. Document findings meticulously to facilitate analysis and reporting, ensuring comprehensive assessment and actionable insights for improving cybersecurity defences.

### TIP 10. SECURE YOUR PRIVATE KEYS IN BLOCKCHAIN SYSTEMS

In safeguarding digital assets within blockchain systems; employing hardware wallets, implementing multi-signature wallets, securely backing up keys, avoiding phishing attacks, and staying updated on security practices are essential. These actions collectively mitigate the risk of unauthorised access and fortify asset security