CHINYELU KARIBI-WHYTE *Cyber Security Consultant Cyb-Uranus Limited*
LinkedIn: https://www.linkedin.com/in/chinyelu-philomena-karibi-whyte/
Website: https://cyburanus.com/ https://pheelpretty.com/

As a cybersecurity enthusiast, Chinyelu specialises in providing tailored security solutions to start-ups and SMEs. With a mission to democratise robust cybersecurity, She blends cutting-edge technology with an unwavering commitment to client empowerment. Her expertise extends to promoting resilience and personal growth, underlining her dedication to both organisational and individual empowerment.

TIP 1: EDUCATE YOUR TEAM ON PHISHING

Train employees to recognise phishing emails. These often contain urgent language and request sensitive information. Encourage verifying through alternative communication before responding.

TIP 2: IMPLEMENT STRONG PASSWORD POLICIES

Require complex passwords that combine letters, numbers, and symbols. Mandate regular password changes every 3-6 months to further protect your systems.

TIP 3: UTILISE MULTI-FACTOR AUTHENTICATION (MFA)

Enhance security by requiring multiple forms of verification before granting access to systems. This simple step can significantly deter cyber attackers.

TIP 4: REGULARLY UPDATE AND PATCH SYSTEMS

Keep all software up to date to protect against vulnerabilities. Regular patches fix security holes that hackers exploit, making this one of the simplest, yet most effective, defences.

TIP 5: SECURE YOUR WI-FI NETWORKS

Ensure your Wi-Fi network is encrypted, hidden, and secure. Avoid using default SSIDs and passwords and consider setting up a separate network for guests. (An SSID (Service Set Identifier) is the name assigned to a Wi-Fi network. When you search for wireless networks to connect to, the names that appear are the SSIDs.)

TIP 6: BACKUP DATA REGULARLY

Regular backups can be a lifesaver in case of data loss or ransomware. Store backups in multiple locations (e.g., cloud and external drives) and test them regularly to ensure they can be restored.

TIP 7: INSTALL ANTIVIRUS SOFTWARE AND FIREWALLS

Use reputable antivirus software and keep it updated. A good firewall acts as a barrier between your data and cyber threats, monitoring and controlling incoming and outgoing network traffic.

TIP 8: LIMIT ACCESS TO SENSITIVE INFORMATION

Operate access controls on a 'need-to-know' basis, to limit who can see sensitive data. This reduces the risk of accidental or malicious data breaches.

TIP 9: SECURE MOBILE DEVICES

With an increasing reliance on mobile devices, ensure that these have secure access to your network. Implement policies

that require devices to be locked with a password or biometric and encrypted if they access business information.

TIP 10: DEVELOP AND TEST AN INCIDENT RESPONSE PLAN

Be prepared for a cyber incident by having an action plan that includes identification, containment, eradication, and recovery steps. Regularly testing your plan ensures that you can respond effectively under pressure.