ARTHUR MAPISA, *Cybersecurity Specialist*
http://www.linkedin.com/in/arthur-m-62b635162
www.interaw.com

"As a freelancer with two years of experience, Arthur brings a proactive approach to cyber security that prioritises prevention, detection, and response. While he may not have extensive years of experience in the field, his dedication to staying updated with the latest security trends, technologies and best practices is unwavering. Arthur actively engages in continuous learning through online courses, certifications, and participation in industry forums to enhance his skills and knowledge.

TIP 1. IMPLEMENT NETWORK SEGMENTATION

Divide your network into smaller segments to limit the spread of malware and unauthorised access, especially in large organisations.

TIP 2. EMPLOY A ZERO-TRUST SECURITY MODEL

Assume that every user, device, and network component is a potential threat and implement strict access controls and verification measures accordingly.

TIP 3. CONDUCT REGULAR SECURITY AUDITS

Perform periodic audits of your systems, networks, and security policies to identify and address any vulnerabilities or weaknesses proactively.

TIP 4. ENCRYPT SENSITIVE DATA

Utilise encryption techniques to protect sensitive information, both in transit and at rest, making it unreadable to unauthorised users; even if intercepted.

TIP 5. MONITOR NETWORK TRAFFIC

Use intrusion detection and prevention systems to monitor network traffic for suspicious activities or anomalies that may indicate a security breach.

TIP 6. PRACTICE THE PRINCIPLE OF LEAST PRIVILEGE

Grant users the minimum level of access and permissions necessary to perform their job functions, reducing the risk of privilege escalation attacks.

TIP 7. SECURE YOUR IOT DEVICES

Change default passwords, update firmware regularly, and segment IoT (Internet of Things) devices on a separate network to prevent them from being exploited as entry points into your main network.

TIP 8. ENGAGE WITH CYBERSECURITY COMMUNITIES

Join online forums, attend conferences, and participate in information-sharing initiatives to exchange knowledge and collaborate with other cybersecurity professionals on emerging threats and defensive strategies.

TIP 9. IMPLEMENT APPLICATION WHITE-LISTING

Allow only approved applications to run on your systems, reducing the risk of malware execution and unauthorised software installations.

TIP 10. HARDEN YOUR INFRASTRUCTURE

Configure servers, routers, and other network devices to follow security best practices and disable unnecessary services or features that could be exploited by attackers.