ANDY HUYNH *Business Analyst*
LinkedIn/Website https://www.linkedin.com/in/andyhuynhwa/

Andy holds a Bachelor of Science with double majors in Networking Security and Business Information Systems. He is currently working as an IT Business Analyst specialising in transformation projects within Cybersecurity and finance, driving significant improvements and innovation in these critical areas.

TIP 1. EDUCATE ON SOCIAL ENGINEERING

My most favourite topic - Train employees to identify and respond to social engineering tactics, such as phishing and pretexting, which are commonly used by attackers to exploit human vulnerabilities. By enhancing awareness and providing practical examples of these tactics, you can empower your team to recognise suspicious activities and avoid falling victim to such schemes. This proactive training is essential for mitigating the risk of breaches caused by human error.

TIP 2. BLOCK USB PORTS OR USE USB PORT CONTROL

USB ports can pose a serious security risk if malicious devices are connected. To mitigate this risk, use port control software to restrict unauthorised access, or completely disable unused ports. This measure helps prevent potential threats from exploiting open USB ports and enhances overall system security.

TIP 3. ENABLE MULTI-FACTOR AUTHENTICATION (MFA)

MFA provides an extra layer of security by requiring users to verify their identity with two or more credentials, reducing the risk of account compromise. This practice should be applied to all employees, not just those with high-level access.

TIP 4. IMPLEMENT GEOFENCING FOR REMOTE ACCESS

Limit remote access to your systems by implementing geographical restrictions, allowing only authorised personnel from specific regions to access sensitive data. This adds an additional layer of security by preventing unauthorised access from unapproved or high-risk locations, helping to safeguard critical systems and information from potential threats originating from outside approved geographical areas.

TIP 5. CONDUCT REGULAR PHISHING SIMULATIONS

Simulating phishing attacks is an effective way to train employees to identify and respond to suspicious emails. By mimicking real-world phishing attempts, these simulations help staff recognise common tactics used by attackers, such as deceptive links or requests for sensitive information. This proactive approach enhances awareness, reduces the risk of security breaches, and encourages prompt reporting of potential threats.

TIP 6. MONITOR CLOUD SHADOW IT

Employees frequently use unapproved cloud services, which can lead to data leaks and compliance issues. Monitoring and managing these services are crucial to prevent such risks. Implementing these lesser-known security tips helps organisations address overlooked vulnerabilities, enhancing their overall security posture and ensuring better protection against potential threats and their data.

TIP 7. REGULAR FIRMWARE INTEGRITY CHECKS

Regularly verify the integrity of firmware on hardware devices such as routers and switches. This proactive measure helps prevent potential security breaches and maintains the reliability and safety of your network infrastructure. Firmware vulnerabilities on routers, printers, and IoT devices are often overlooked, making them exploitable targets.

TIP 8. REGULARLY TEST YOUR INCIDENT RESPONSE PLAN

An untested incident response plan might fail during a real attack. To ensure your team can respond effectively, conduct regular drills and simulations. These exercises help identify weaknesses, refine procedures, and improve coordination, ensuring that your response plan is robust and ready when a real incident occurs. Regular practice is crucial for maintaining readiness and effectiveness.

TIP 9. IMPLEMENT LEAST PRIVILEGE PRINCIPLES

Grant users only the minimum level of access necessary for their job. This approach limits potential damage if an account is compromised, as users are restricted to only the resources they need. By minimising access, you reduce the attack surface and enhance overall security.

TIP 10. DATA PRIVACY REGULATIONS

Ensure compliance with data privacy regulations like GDPR and CCPA by implementing robust data protection measures. Regularly audit data handling practices, secure personal data through encryption, and establish clear policies for data access and retention. Additionally, train employees on data privacy requirements and respond promptly to data breaches to mitigate risks and avoid significant fines for non-compliance.