CHIOMA CHIGOZIE-OKWUM, *Director of ICT, Spiritan University Nneochi, Abia State, Nigeria.*
https://www.linkedin.com/in/chioma-chigozie-okwum-376793122/

Chioma Chigozie-Okwum, indigenous to Nigeria, is a cyber security researcher, educator, content creator and advocate. Chioma is a serial tech enthusiast and is passionate about cyber safety awareness propagation, which has earned her many national and international recognitions. She is pursuing cyber-psychology and human factor security frontiers.

TIP 1: CYBER SECURITY IS EVERYONE'S BUSINESS

It is good practice for enterprises to ensure that all staff members understand how much cyber security is everybody's business. This will ensure that everyone from top management, through finance, human resources to the doorman, understands what risk their actions (and inactions) can pose to your enterprise. Everyone should be prepared to take responsibility.

TIP 2: QUALITY ASSURE VENDORS AND 3RD PARTY PARTNERS

It is good practice to quality assure and secure proof that the cyber security policies, plans, compliance and regimes of all vendors and 3rd party service providers are in place. This is very vital to ensure that the security vulnerabilities of vendors and partners are not exploited by potential cyber threats.

TIP 3: UPDATE INFRASTRUCTURE

Outdated software and hardware have been identified as vulnerability points, as such outdated infrastructure lack the security patches implemented during updates. It is cyber security best practice to ensure that all software and hardware are updated and running the most current version to eliminate loose ends being potentially exploited by cyber threats.

TIP 4: HAVE A ROBUST CYBER SECURITY TRAINING PLAN

The importance of training, and retraining, of all personnel on cyber security plans, policies and procedures in every enterprise cannot be over emphasised. Training of staff on the latest cyber safety best practices should be periodic, and the training should be scaled to address the needs of every individual employee.

TIP 5: ENSURE ALL PAYMENT TERMINALS ARE FOOL PROOF

Point of sales terminals are usually a target point in small- and medium-scale enterprises. It is therefore very important that all payment terminals are monitored and secured to ensure that they are not hacked into and customers' details are not harvested through them, and to avoid any resulting loss of enterprise reputation.

TIP: 6 MINIMISE CHANCES OF BREEDING MALICIOUS INSIDERS

One of the weakest security links in any enterprise are malicious insiders; these can range from disgruntled, unsatisfied, poorly appreciated and even uninformed insiders. It is best practice to ensure that all employees are treated fairly to eliminate breeding a workforce that can turn malicious and potentially aid cyber threats.

TIP 7: MITIGATE AGAINST COMPLACENCY

Adhering to cyber security procedures religiously is a way of mitigating against creating loopholes that could potentially lead to cyber attacks. Employees are usually enthusiastic in the beginning, but can grow complacent over time, it is therefore important to monitor and eliminate complacency while using technology and AI. Rewards can be given to encourage compliance.

TIP 8: INSTIL AND SUSTAIN A STRONG CYBER SECURITY CULTURE

It is very vital to grow and sustain a very strong cyber security culture within the enterprise. This is achieved by quality assuring all cyber security processes. It is vital to keep reminding staff of their commitment to security using multimedia channels and deployment of simulated hacks to test compliance.

TIP 9: MONITOR AND ASSESS RISKS

It is vital to monitor and assess all possible cyber risks. The risk assessment should be done using both qualitative and quantitative methods to provide insights on the dangers posed by the risks, as well as the level of loss they could cost the enterprise. Investment in SIEM (Security Information Event Management) tools is advocated.

TIP 10: HAVE A STRONG PASSWORD POLICY

Password policies in enterprises stipulate the regimes surrounding creating and using passwords. This also ensures that all platforms accept strong passwords. Employees often feel negligent towards password policies. It is vital to monitor and enforce strict compliance to password policies leveraging on technology.