SALMAN ABIOLA SULEIMAN (SAS) *Security Associate, RepConsults UK.| Founder ;Meta0lopa*
LinkedIn.com/in/Salman-Sas

Salman is an expert, with keen interest in data protection and fraud mitigation at scaled and enterprise level. He is exceptionally customer focused and result oriented.

TIP 1. TEACH EMPLOYEES ABOUT SECURITY REGARDLESS OF THEIR POSITION

Always make sure you show employees how to identify scam and bad fake emails to let them be at alert for events with frauds. Holding periodic training classes to help them understand the concepts in a fun and easier approach. These sets of knowledgeable employees will be the first line to defend against any attacks in future.

TIP 2. USE ONLY SECURE PAYMENT SYSTEMS FOR TRANSACTION

Use only the secure connections for the payment gateways and routinely update and patch these payment systems. These will help to protect the customers' payment information and privacy while building trust and good reputation. Transactions will indeed have an end to end protection while ensuring that each customer is not at risk of losing data or funds.

TIP 3. CREATE AN ACCESS LIMIT TO SENSITIVE INFORMATION

Important data and files should only be accessed by those employees who are in need of it at a specific time frame. Sensitive information should have a certain hierarchy to ensure company files are separated from day to day reoccurring ones. There should be a regular update and review to reduce the potential risk for leaks and other insider threats.

TIP 4. UTILISE A SECURED WIRELESS NETWORK

Wi-Fi should be secured with strong password and good encryption, rather than using default manufacturer settings. The settings for security and protection should be updated regularly to prevent illegal and unauthorised access to the network by intruders. The best way to ensure safety with the network is to make sure the personnel in charge have the interest of the safety of the company at heart, rather than just working for hours.

TIP 5. MONITOR FOR STRANGE ALERTS

Effective monitoring tools at enterprise level should be used to watch for strange activities like data and network breaches, or file configurations. Adequate action should always be followed to fix any problems that might arise from the various set of rules and alerts to ensure safe operation at each working schedule.

TIP 6. MULTI-FACTOR AUTHENTICATION IS YOUR FRIEND (MFA)

Multi-factor authentication is best for extra layer security, rather than passwords. MFA should not only be turned on for apps being used in the premises alone; but they should also be implemented for all enterprise accounts and associated accounts . This will ensure you can only log in with a code sent to the authorised phone before having access to the app or service.

TIP 7. USE SECURITY PLUG-IN FOR THE ONLINE STORE

Online store and shops have always been a target for attacks, So the use of an extra security plug-in from TRUSTED vendors to keep the account safe is important. This can be energised by using strong passwords and encouraging customers to follow best ethics by avoiding the use of the same password for multiple accounts.

TIP 8. ENCOURAGE TRUSTED ANTI-VIRUS AND ANTI-MALWARE SOFTWARES

All devices should have an anti-virus installed, with appropriate licence for the version currently been used by each user. These should be updated regularly from ONLY the OFFICIAL vendors rather than a pirated version to cut costs. Incidences with virus can only be prevented when there's an adequate use of the antivirus software, with monitored interval checks to ensure optimum safety.

TIP 9. EMBRACE CLOUD AND DATA BACK UP TECHNIQUES

DATA are the essentials for all operations to function properly. Cloud services and the use of external secured drive should be used to store important data. This data can easily be recovered in short time when an attack happens, or in the case where a set of system files got infected. This will help restore to a decent considerably stable state.

TIP 10. PLAN FOR INCIDENTS AND RUN SIMULATIONS

PLAN before the problem. It is always super helpful to plan before things go wrong and know who to contact for data recovery - and actions needed to fix issues quickly. Performing targeted drills would also prepare the mindset for any common related events that could affect the company structures and limit proper functioning.