Staff Cybersecurity Awareness

By KAGGA PIUS

Cybersecurity awareness is a type of education that teaches employees on how to identify, prevent and respond to cyber threats.

Here’s a breakdown of the different levels of cybersecurity focusing on the scale of implementation

- Personal level: This refers to the cybersecurity practices individuals/employees take to protect their devices and data. such as device security, data protection, social media security.

Cont.

- Organizational level: This involves businesses, institutions, organizations and other companies to protect their systems and data.

  NOTE: This builds upon individual user practices and adds layers of protection

  This practices include; Network security, Access Controls and Incident Response Planning.

Cont.

- Government Level: This is the broadest level, encompassing on national security strategies. Governments play a crucial role in developing cyber regulations, information sharing & cyber defense

Focusing on the

Organizational level

Information and **Systems**

Organization Information(InfoSec)

Organizational Information refers to any data that pertains to the functioning and identity of an Organization. For example:

- Basic Information
  (Name and legal structure, Contact Information, leadership information)
- Operational information
  (mission and Vision statements, Financial information & products and services)

Cont.

- Regulatory Information
  (Industry-Specific licenses and permits, Compliance Policies)

- Internal Information (For Authorized Users)
  (Employee information, Project-management information,
  Customer relationship management data)

Organization Information(InfoSec)

Information Security is the practice of protecting information from unauthorized access, use, disclosure, disruption, modification or destruction.

There are number of tools and processes designed to safeguard sensitive information whether it is electronically, physically or transmitted across networks.

Objectives of Information(InfoSec)

The core objectives of InfoSec are based on “CIA TRIAD”.

Confidentiality: Ensuring only authorized users have access to information.

Integrity: Maintaining the accuracy and completeness of information.

Availability: Guaranteeing that authorized users can access information when needed.

Organization systems security

Systems Security is a subset of information security that specifically focuses on protecting computer systems and networks from unauthorized access, use, modification or destruction. System security acts as a shield around a castle, designed to keep your data safe by securing the underlying infrastructure.

Organization systems security

System security primarily deals with hardware, software and network components that make up the organization’s computer systems and aims to ensure that “CIA TRIAD” of information is stored, processed or transmitted within those systems.

The core elements of systems security include: network security, operating systems security, application security, endpoint security, data encryption.

Cyber threats faced by

Organizations

Attackers and **Attacks**

Cyber Attackers / Hackers

A cyber attack is the process of attempting to steal data or gaining unauthorized access to computers and networks using one or more computers.

A cyber attacker /hacker(s) are people or group who attempt to exploit the vulnerability for personal or financial gains

Types of Cyber Attackers / hackers

a) Amateurs (script kiddies)
b) Hackers (Black hat, White hat & Grey hat)
c) Organized Hackers (Cyber criminals, Hacktivists, cyber terrorists & state-sponsored hackers)

Types of Cyber Attacks

A Cyber attack is essentially a digital assault, Hackers usually employ various methods to breach an organization, business, company's systems with an aim of stealing sensitive data, disrupting critical infrastructure whereas financial gain.

NOTE: No one is immune and cyber attacks are constantly evolving.

Types of Cyber Attacks

These include;

- Spy-ware: Designed to trade and spy on you.
- Adware: Designed to automatically deliver advertisements to a user most often on a web browser.
- Backdoor: Used to gain unauthorized access by passing the normal authentication procedures.
- Ransomware: Designed to hold a computer system or it's data it contains captive until a payment is made.
- Trojan Horse: carries out malicious operations by making itself true.

Cont.

- Scareware: Uses scare tactics to trick you into taking a specific action:
- Rootkit: Designed to modify the operating system to create a back door for which attackers can use to access your computer remotely.
- Virus: a computer program that when executed, replicates and attaches itself to either executable files such as a document.
- Worms: replicates itself in order to spread from one computer to another unlike a virus requires a host program to run

System symptoms of Cyber Attacks/malware

- An Increase in CPU usage which slows down the computer.
- Computer freezing and crashing most often
- A decease in web browsing speed
- Unexplainable problems with your network connections
- Modified/deleted files
- Emails sent without your consent or knowledge

Whew!
You made it.

In your role within the organization, how can you contribute to a culture of information security awareness.

What specific action will you take to improve your information security practices when handling sensitive data.