Cyber Security Basics: CompTIA A+ Foundations: Hardware, Software, Networking & Security Essentials

Learning Outcomes: Participants will be able to:

- Identify and assess digital threats and vulnerabilities.
- Implement cybersecurity tools and security protocols.
- Apply best practices in ethical hacking, compliance, and risk management.
- Configure secure systems and networks, including Windows and cloud environments.
- Demonstrate readiness for practical cybersecurity roles and certifications.

Mode of Delivery:
This program is delivered fully online via weekly modules including hands-on labs, virtual simulations, discussion-based learning, and instructor-led synchronous sessions.

Week	Focus/Topic	Assignments/Tasks
1- Introduction to IT & Mobile Devices	Learners will identify common mobile device components and connectivity standards to understand their roles in IT environments.	Label a mobile device teardown (diagram-based)
		Discussion: Mobile device impact on work/life
		Virtual disassembly resources (iFixit, videos, PDFs)
2- Hardware Interfaces & Peripheral Devices	Learners will classify various hardware components, cables, and peripheral devices based on their functions and compatibility with different systems.	Cable/port matching game
		Diagram a desktop setup with labeled ports
		Upload a narrated screencast walking through the physical parts of a desktop or laptop.
3- Networking & Wireless Communication	Learners will explain fundamental networking concepts, protocols, and	Network simulator (Cisco Packet Tracer or

	wireless standards used in local and internet-based communications.	Diagrams.net)
		IP configuration and DNS worksheet (with screenshot prompts)
4- Operating Systems Essentials (Windows + Others)	Learners will compare features of major operating systems and demonstrate the use of system tools and utilities within Windows and macOS environments.	Windows interface scavenger hunt (virtual lab)
		OS comparison chart (features, use cases)
5- Troubleshooting Foundations	Learners will apply the troubleshooting process to diagnose and resolve basic hardware, software, and peripheral issues.	Simulate a user ticket and write a step-by-step resolution
		Practice with Windows tools (e.g., SFC, disk cleanup)
6- Security Concepts and Practices	Learners will analyze common security threats and implement preventive strategies using physical and logical security controls.	Simulated phishing email analysis
		Security checklist for a SOHO setup
7- Windows Security and System Tools	Learners will configure Windows security tools and permission settings to ensure device and data protection.	Configure firewall rules (screen demo)
		Security misconfiguration case study
8- Virtualization, Cloud & Mobile Security	Learners will demonstrate the setup of virtual environments and differentiate between cloud computing models and mobile security practices.	Cloud comparison matrix
		Use Oracle VirtualBox to install a Linux VM (guided lab)
9- Operational Procedures & Scripting Basics	Learners will develop basic scripts and implement IT operational procedures such	Write and test a basic script to automate a task (e.g., file backup)

	as documentation, remote access, and system backups.	Role-play: help desk call scenario
10- Certification Preparation & Capstone	Learners will evaluate their readiness for the CompTIA A+ certification through practice exams and a hands-on capstone troubleshooting project.	Capstone: Complete a simulated IT support case (hardware + OS + security)
		Take a full CompTIA A+ practice test
		Submit a study plan + confidence rating by domain