LESSON PLAN

COURSE OUTLINE

CYBERSECURITY-FOUNDATION

OVERVIEW OF BEGINNER LEVEL CYBER SECURITY

There has never been a better moment to study cybersecurity than right now. Because of the significance in this day and age, systems, data, and information are continuously under attack, and tech workers and managers must be able to stay aware of and apply the latest technologies and tactics to protect their important data from falling into the wrong hands. Enroll in our cyber security instructed-led online course to learn the terminologies, technical know-how, and practical skills needed to combat threats. Get hands-on experience and technical knowledge to protect your digital assets. Learn about numerous attack kinds and how to combat all aspects of a company's technology and commercial processes. Make sure your skills are up to date and your systems are effectively protected in the fierce struggle for information security.

OBJECTIVE OF THE COURSE

This course aims to:

- Make you understand why you should take Cybersecurity seriously.
- Teach how simple it is to secure your devices. And how this can prevent attacks and make your devices more secure.
- Teach participants what Social Engineering is and how the hackers are using it. What the most common forms of Social Engineering are.
- Teach participants how to protect the personal data you have recorded on your computers, laptops and mobile devices.
- Make you job ready if you need to pursue a career in cybersecurity.

LEARNING OUTCOME

- Protect and defend computer systems and networks from cybersecurity attacks.
- Diagnose and investigate cybersecurity events or crimes related to computer systems and digital evidence.

- Apply critical thinking and problem-solving skills to detect current and future attacks on an organization's computer systems and networks.
- Effectively communicate in a professional setting to address information security issues.

WHO THIS COURSE IS MEANT FOR?

- Anyone with a keen interest in information and internet security/safe practices.
- Everyone who is using electronic devices like computers, laptops and mobile phones.

DETAILED COURSE CONTENT

- Neo Cloud Technologies offers Professional Training in Cybersecurity from beginner level through intermediate to professional

COURSE REQUIREMENT

- Basic knowledge of Computer Fundamentals.

WEEK 1: Introduction to Cyber Security

- Introduction to Cyber Security
- The Need of Cybersecurity
- Introduction to Personal Data
- Your Online and Offline Data
- Where is your Data
- Your Computing Devices
- The Cyberspace
- Introduction to Organizational Data
- Confidentiality, Integrity and Availability
- Lab: Compare Data with a Hash
- The Impact of a security Data
- The Profile of a Cyber Attacker: types of attackers
- What is Cyberwarfare
- The Purpose of Cyberwarfare
- Revision
- Test Your Knowledge: Sample Questions

WEEK 2: Cyber crimes
Subtopic: Attacks, Concepts and Techniques

- Types of Cyber Crimes
- Attacks, Concepts and Techniques
- Hacktivists, Cyber Terrorists, Cyber Criminals, Countries
- Security Vulnerabilities and Exploits
- Types of Malware and Symptoms
- Methods of Infiltration
- DoS, DDoS and SEO
- Blended Attack
- Impact Reduction
- Test Your Knowledge: Sample Questions

WEEK 3Networking Basics

- The Open System Interconnection (OSI) Model
- The TCP/IP Model
- Comparing the OSI and TCP/IP Models
- TCP Handshake and TCP Flags
- Private IP and Public IP
- Port Numbers
- IP V6 Basics

- MAC Addresses
- Introduction to DNS
- Dynamic Host Control Protocol
- ARP: Address Resolution Protocol
- Network Address Translation: NAT
- Access Control Lists: ACL
- VPN (Remote Access VPN, Site-to-Site VPN)
- Common Network and Network Security Devices
- Routers and Switches
- Firewall, IDS, and IPS
- Test Your Knowledge: Sample Questions

WEEK 4: Virtualization and Cloud Basics

- What Is Virtualization?
- Hypervisors
- The Type 1 Hypervisor
- Type 2 Hypervisor
- Commonly Used Hypervisors
- Snapshots
- Common Security Issues with Virtual Machines
- Creating a New Virtual Machine with Oracle VirtualBox
- Software Containerization with Docker
- Cloud Computing
- Types of Cloud
- Cloud Service Offerings
- Benefits of Using the Cloud
- Cloud Security Considerations
- Test Your Knowledge: Sample Questions

WEEK 5: Programming Basics for Security Enthusiasts

- Windows PowerShell
- The PowerShell Integrated Scripting Environment
- For Loops
- Pipes
- File-Handling Functions
- Web / Networking Functions
- Linux Shell Scripting
- Structural Basics of a Shell Script
- Creating Your First Shell Script
- Reading Input from the User
- Logic Building

WEEK 6: Information Security Basics

- Understanding the Basics: Confidentiality, Integrity and Availability
- Common Challenges in Implementing Information Security Controls
- Authentication, Authorization, and Accounting (AAA)
- Information Security Terminology
- What Is Nonrepudiation?
- What Is a Vulnerability?
- What Is a Zero-Day Vulnerability/Exploit?
- What Is an Exploit?
- What Is a Risk?
- What Is a Threat?
- Putting It All together: Vulnerability, Risk, Threat, and Exploit
- Information Security Threats
- Types of Hackers
- What Is the Difference between Hacking and Ethical Hacking?
- Policy, Procedure, Guidelines, and Standards
- Incident Management
- Test Your Knowledge: Sample Questions

WEEK 7: Accounts, Credentials and Identity thefts

- Dictionary Attack and Brute Force
- Password Security
- Personal Accounts Breach
- Personal Accounts Recovery
- Email Accounts
- Identity Theft
- Test Your Knowledge: Sample Questions

WEEK 8: Privacy essentials

- Photo Metadata
- Geolocation
- Seeking Privacy on the Internet
- Fictive Accounts & Credentials
- Your Document's Metadata
- Deleted Data
- Hiding your IP
- Private Search Engines
- Tor
- Browsing Digital Traces
- Test Your Knowledge: Sample Questions

WEEK 9: Safe browsing

- Web Exploits
- HTTPS, Digital, Certificates and Encryption
- Cookies
- Web Browsers
- Advanced Tools
- Test Your Knowledge: Sample Questions

WEEK 10: Information Gathering

- What is Footprinting?
- What is Enumeration?
  Test Your Knowledge: Sample Questions

WEEK 11: Cryptography

- Cryptography and Its Objectives
- Types of Cryptography
- Symmetric Encryption
- Asymmetric Encryption
- Key Escrow
- Types of Ciphers
- Cryptography Tools
- Message Digests
- Secure Shell (SSH)
- PKI
- Common PKI Terminology
- Components and Types of an SSL Certificate
- Testing an SSL Certificate
- Digital Signatures
- SSL and TLS
- Data That Can Be Encrypted
- Attacks on Cryptography and Cryptanalysis
- Test Your Knowledge: Sample Questions

WEEK 12: Project

MODE OF LEARNING: Online

WHO ARE THE LECTURERS?

This course will be taught by Neo Cloud Technologies Certified Cyber Security Expert.

LENGTH OF THE COURSE

12 Weeks – Mon., Wed., Fri.

ASSESSMENT AND CERTIFICATION

- **Mid-term assessment: Written exam covering weeks 1-6**
- **Final assessment: Practical exam and case study covering weeks 7-12**
- **Certificate of Completion awarded to participants who successfully complete the course.**