FUTURE PROOF LEARNING - NEP ALIGNED
www.mycreditcourses.com

CERTIFIED SECURE COMPUTER USER

DURATION: 60 Hours
CREDITS: 2

COURSE SYLLABUS

Objective

The CSCU training program aims at equipping the students with the necessary knowledge and skills to protect their information assets. The program is designed to interactively teach the students about the whole gamut of information security threats they face ranging from identity theft and credit card fraud to their physical safety. The skills acquired during the course of this program will not only help the students to identify these threats but also to mitigate them effectively.

Exit Profile

- Respond to Cybersecurity Incidents:
- Cybersecurity Awareness
- Protect Personal and Professional Data
- Ensure Safe Online Practices

Career Path

- Cybersecurity Assistant
- Technical Support Representative
- Junior Systems Administrator
- Network Support Technician
- IT Support Technician
- Security Awareness Trainer
- Personal Security Consultant

Course Outline

Course Name:	CERTIFIED SECURE COMPUTER USER	Duration: 60 H	
Module	Topic	Duration	Total Duration
Module - I	INTRODUCTION TO SECURITY	4	20 H
	SECURING OPERATING SYSTEMS	6	
	MALWARE AND ANTIVIRUS	5	
	INTERNET SECURITY	5	
Module - II	SECURITY ON SOCIAL NETWORKING SITES	4	22 H
	SECURING EMAIL COMMUNICATIONS	6	
	SECURING MOBILE DEVICES	6	
	SECURING THE CLOUD	6	
Module - III	SECURING NETWORK CONNECTIONS	5	18 H
	DATA BACKUP AND DISASTER RECOVERY	5	
	SECURING IOT DEVICES AND GAMING CONSOLE	4	
	SECURE REMOTE WORK	4	

Course in Detail

MODULE: 1

INTRODUCTION TO SECURITY

- Data–Digital Building Blocks
- Importance of Data in the Information Age
- Threats to Data
- Data Security
- Potential Losses Due to Security Attacks
- Implementing Security

SECURING OPERATING SYSTEMS

- Guidelines to Secure Windows
- Guidelines to Secure Mac OS

MALWARE AND ANTIVIRUS

- What is Malware
- Types of Malware
- Symptoms of Malware Infection
- Antivirus
- Configuring and Using Antivirus Software
- How to Test If an Antivirus is Working

INTERNET SECURITY

- Understanding Web Browser Concepts
- Understanding IM Security
- Understanding Child Online Safety

MODULE: 2

SECURITY ON SOCIAL NETWORKING SITES

- Understanding Social Networking Concepts
- Understanding Various Social Networking Security Threats
- Understanding Facebook Security Settings
- Understanding Twitter Security Settings

SECURING EMAIL COMMUNICATIONS

- Understanding Email Security Concepts
- Understanding Various Email Security Threats
- Understanding Various Email Security Procedures

SECURING MOBILE DEVICES

- Understanding Mobile Device Security Concepts
- Understanding Threats to a Mobile Device
- Understanding Various Mobile Security Procedures
- Understanding How to Secure iPhone and iPad Devices
- Understanding How to Secure Android Devices
- Understanding How to Secure Windows Device
- Mobile Security Tools

SECURING THE CLOUD

- The Concept of Cloud
- How Cloud Works
- Threats to Cloud Security
- Safeguarding Against Cloud Security Threats
- Cloud Privacy Issues
- Addressing Cloud Privacy Issues
- Choosing a Cloud Service Provider

MODULE: 2

SECURING NETWORK CONNECTIONS

- Understanding Various Networking Concepts
- Understanding Setting Up a Wireless Network in Windows
- Understanding Setting Up a Wireless Network in Mac
- Understanding Threats to Wireless Network Security and Countermeasures
- Measures to Secure Network Connections

DATA BACKUP AND DISASTER RECOVERY

- Data Backup Concepts
- Types of Data Backups
- Windows Backup and Restore Procedures
- MAC OS Backup and Restore Procedures
- Understanding Secure Data Destruction

SECURING IOT DEVICES AND GAMING CONSOLE

- What are IoT Devices?
- What are Gaming Consoles?
- Why Security is Important?
- Common Security Threats
- Basic Security Measures
- Secure Network Practices
- Monitoring and Managing Devices
- Device-Specific Security Tips

SECURE REMOTE WORK

- What is Remote Work?
- Why Remote Work Security is Important?
- Common Security Risks for Remote Workers