

training code: CSCU / ENG DL 2d / EN

Certified Secure Computer User

Certified Secure Computer User

The purpose of the authorized **EC-Council CSCU - Certified Secure Computer User** training program is to provide individuals with the necessary knowledge and skills to protect their information assets. This class will immerse students into an interactive environment where they will acquire a fundamental understanding of various computer and network security threats such as **identity theft**, online **banking phishing scams**, **credit card** fraud, backdoors and **viruses**, emails hoaxes, sex offenders lurking online, loss of confidential information, **hacking attacks** and **social engineering**. 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. More importantly, the skills learned from the class helps students take the necessary steps to mitigate their security exposure.



Purpose of the training

This **course** is specifically designed for today's computer **users** who use the internet and the www extensively to work, study and play.



Benefits of completing the training

The courseware comes complete with demo videos and scenario-based discussion questions to allow the student to gain actual skills.

- Raising **awareness** of threats related to the activities of cybercriminals
- Reducing the **risk** of confidential data theft or phishing
- Lowering the risk of business process continuity loss
- Protection of the organization's ICT infrastructure

As part of the training, participants receive a voucher for the **CSCU** exam **112-12** to verify the acquired knowledge and skills

This certification is an excellent complement to educational offerings in the domain of security and networking.



Exam description

EXAM DETAILS:

Number of Questions: 50

Passing Score: 70%

Test Duration: 2 Hours

Test Format: Multiple Choice

Test Delivery: EC-Council Exam Portal



Expected Listener Preparation

Basic computer skills



Training Language

- Training: English
- Materials: English



Training Includes

Voucher for the CSCU **exam** (112-12)

Duration

2 days / 14 hours

Training agenda

1. Introduction To **Data Security**
 - 1.1 How Often Do We Generate Data
 - 1.2 **Threats** to Data
 - 1.3 Data Security
 - 1.3.1 Why Do We need Data Security
 - 1.4 Potential Losses Due to **Security Attacks**
 - 1.4.1 **Financial Loss**
 - 1.4.2 Unavailability of Resources
 - 1.4.3 **Identity Theft**
 - 1.4.4 Loss of Trust
 - 1.5 Implementing Security
2. Securing Operating Systems
 - 2.1 Guidelines To Secure Windows
 - 2.1.1 Disable the Guest Account
 - 2.1.2 Lock Out Unwanted Guests
 - 2.1.3 Disable Jump Lists
 - 2.1.4 Adding New Apps In **Firewall**
 - 2.1.5 Creating a New Firewall Rule
 - 2.1.6 Turn on **Windows Defender**
 - 2.1.7 Enable **bitlocker**
 - 2.1.8 Killing Unwanted Processes
 - 2.1.9 How To **Hide Files and Folder**
 - 2.2 Guidelines To **Secure Mac OS X**
 - 2.2.1 Disable Automatic Login
 - 2.2.2 Disable Guest Account
 - 2.2.3 Enable FileVault
 - 2.2.4 Enable Firewall
 - 2.2.5 Enable and Set **Parental Controls**
3. Malware and Antiviruses
 - 3.1 **Viruses**

3.2 Trojans

3.3 Symptoms Of **Malware Infection**

3.4 How Does **Antivirus** Work

3.4.1 How Does an Antivirus Deal With an Infected File

3.4.2 How to Choose The Right Antivirus Software

3.5 Configuring and Using Antivirus Software

3.6 How To Test If an Antivirus is Working

4. Internet Security

4.1 Securing the **Web Browser**

4.2 Identify a **Secure Website**

4.3 Understanding IM Security

4.3.1 Determining if Children are at Risk Online

4.3.2 **Protecting Children** from Online Threats

4.3.4 How to Report a Crime

5. Security On Social Networking Sites

5.1 Understanding Various **Social** Networking Security **Threats**

5.1.1 Security Risks Associated with Social Networking Sites

5.1.2 Geotagging

5.3 **Facebook Privacy** and Security Settings

5.3.1 Privacy Settings for Applications

5.3.2 Recommended Actions for Facebook Search Settings

5.4 Understanding **Twitter Security** Settings

6. Securing Email Communications

6.1 Key Considerations While Choosing an Email Client

6.2 Understanding Various **Email Security** Threats

6.2.1 **Malicious** Email **Attachments**

6.2.2 Malicious User Misdirection

6.2.3 Email Attachments: Caution

6.2.4 Email Security Threats: **Phishing**

6.2.5 Email Security Threats: Hoax Mail

6.2.6 Nigerian Scam

6.2.7 **Anti-Spamming** Tool: SPAMfighter

6.3 Scan Email Attachments for Malware

6.4 Check for Last Account Activity

6.5 **Digitally Sign** Your Emails

6.6 **Encrypt** Your **Mails**

6.7 Email Security Tools

7. Securing Mobile Devices

7.1 Understanding Mobile Device Security Concepts

7.1.1 Importance of **IMEI** Number

7.2 **Mobile Malware**

- 7.2.1 Mobile Application Vulnerabilities
- 7.2.2 **Threats** to **Bluetooth** Devices
- 7.2.3 Updating Applications in **Android** Devices
- 7.3 Updating Applications in **iOS** Devices
 - 7.3.1 Install Mobile Phone Antivirus
 - 7.3.2 Securing Bluetooth Connectivity
 - 7.3.3 **Securing Wi-Fi** Connectivity
- 7.4 Understanding How to Secure **iPhone** and **iPad** Devices
- 7.5 Understanding How to Secure Android Devices
- 7.6 Understanding How to Secure **Windows** Device
- 8. Securing The Cloud
 - 8.1 Threats To **Cloud Security**
 - 8.1.1 Disgruntled Insider
 - 8.2 Safeguarding Against Cloud Security Threats
 - 8.2.1 Back Up Data
 - 8.3 Addressing **Cloud Privacy** Issues
 - 8.3.1 Questions to Ask Before Choosing a Service Provider
- 9. Securing Network Connections
 - 9.1. Steps for **Home Networking**
 - 9.2 Understanding Setting Up a **Wireless Network** in Windows
 - 9.3 Understanding Setting Up a Wireless Network in Mac
 - 9.4 Understanding Threats to Wireless Network Security and Countermeasures
 - 9.4.1 Securing Wireless Network
 - 9.5 Measures to Secure Network Connections
- 10. Data Backup and Disaster Recovery
 - 10.1 Data Backup Concepts
 - 10.1.1 What Files to Backup and How Often
 - 10.2 Windows **Backup** and **Restore** Procedures
 - 10.3 MAC OS X Backup and Restore Procedures
 - 10.3.1 Restoring Files from **Time Machine** Backups
 - 10.4 Why Do We Need to Destroy Data Permanently?