



Course Outline Version 1

Foundations of Security

- Essential terminology
- Defining security
- Need for security
- Cyber crime
- Information Security statistics
- IS triangle
- Security myths
- How to harden security

Basic Security Procedures

- Why do I need to worry about my computer's security?
- Introduction
- Hardening of Operating System
- Updating the system and configuring the updates
- Disable unnecessary services
- Strong password creation
- Deployment of antivirus and firewall
- Disable guest account access
- "Make Private" folders
- Security settings in MS Office applications

Desktop Security

- What is file sharing?
- Types of file sharing
- How to share folder?
- Configuring shared folder permissions
- Hiding files and folders
- File sharing tips
- File downloading tips
- How to backup data and restore?
- How to encrypt and decrypt files?
- How to kill suspect processes?

Administering Windows Securely

- How to use the event viewer?
- How to enable auditing in windows?
- How to read logs on your system?
- How to close ports?
- Overview of the windows registry
- How to restore the registry?
- How to close a port?
- Common internal commands
- How to find services and ports they listen on?

Recognizing Security Threats and attacks

- Phishing and its countermeasures
- Virus
- Trojan Horse
- Worms
- Spyware
- Adware
- Keylogger
- Social engineering
- Denial of Service
- Spamming
- Port Scanning
- Password cracking
- Basic security measures

Secure Internet Access

- Basic browser security settings
- How to restrict site access
- Removing site from security zone
- Secure website detection
- Secure site and browser properties
- Tools: Internet Filtering Software
- Configuring Internet content access
- Activating Content Advisor
- How to deal with cookies
- Using P2P networks securely
- Choosing appropriate browser settings
- Wireless network security features

Working on the Internet

- Precepts of Security
- Knowing Encryption
- Digital Certificate
- Digital Signature
- Working with e-mail (web based)
- Working with e-mail (mail client)
- Working with File Transfer- FTP
- Working with File Transfer – Web Folders

Knowing Online Payment Systems

- Working with Credit Cards
- Working with Instant Messengers
- Working across File Sharing Networks
- Working on Dial-in Networks
- Working with Portable Devices
- Working with Wireless Devices
- Working with USB devices
- Working with Media Files
- Working with 3rd party software

Incident Response

- What is Incident Response?
- Incidents and responses:
 - Trojan attack
 - Boot sector virus attack
 - Corrupted registry
 - Automatic running of CD-ROM (autorun.inf)

Prerequisites:

Basic computing skills like browsing the web and checking e-mails.

Who Should Attend:

- Office knowledge workers
- Home users
- Any non-IT person using computers in their office

Schedule:

Please visit EC-Council's Accredited Training Centers to find all of our upcoming classes, dates and locations.

Duration:

2 days (9:00 - 5:00)