C|SCU
Certified | Secure Computer | User

Certified Secure Computer User

Course Outline (version 2)

EC-Council

Hackers are here. Where are you?

CERTIFIED SECURE COMPUTER USER

This course is aimed at end users in order to educate them about the main threats to their data's security. It also equips the students with the basic knowledge that helps them to keep their devices and data secure in daily life. It teaches basic techniques of being secure both online and offline.

COURSE OBJECTIVES

After successfully completing this course, students will be able to:

- Understand the need and importance of data security.
- Implement Operating System security measures on their computers.
- Understand Malware and its symptoms.
- Make an informed decision about choosing the antivirus which is most relevant to their needs.
- Understand the risks associated with different online activities.
- Understand why and how to secure web browsers.
- Identify safe websites.
- Safeguard against the threats associated with online social networking.
- Understand how to make their social networking accounts secure.
- Understand the threats associated with email communications and how to safeguard against them.
- Understand the threats to mobile devices and how to safeguard against them.
- Understand the threats associated with cloud accounts and how to safeguard against them.
- Make an informed decision about a cloud service provider which fulfills their requirements.
- Understand the various types of networks and the threats associated with them.
- Configure a home network.
- Make their networks secure.
- Understand the threats to data and the need for data backups.
- Back up and restore data on their computers.
- Destroy data permanently.

MODULE	TOPIC	DETAILS
1. Introduction To Data Security	1.1 Data–Digital Building Blocks	1.1.1 What is Data 1.1.2 How Often Do We Generate Data 1.1.3 Data Vs. Information
	1.2 Importance of Data in the Information Age	1.2.1 Importance of Personal Data 1.2.2 Importance of Organizational Data
	1.3 Threats to Data	1.3.1 Natural Threats 1.3.2 Threats to Your Data From You 1.3.3 Threats to Your Data From Others
	1.4 Data Security	1.4.1 What is Data Security 1.4.2 Why Do We need Data Security 1.4.3 Elements of Security
	1.5 Potential Losses Due to Security Attacks	1.5.1 Financial Loss 1.5.2 Unavailability of Resources 1.5.3 Identity Theft 1.5.4 Loss of Trust 1.5.5 Data Loss/Theft 1.5.6 Misuse of Computer Resources
	1.6 Implementing Security	1.6.1 Precaution 1.6.2 Maintenance 1.6.3 Reaction
2. Securing Operating Systems	2.1 Guidelines To Secure Windows	2.1.1 Lock the System When Not In Use 2.1.2 Create a User Account Password 2.1.3 Change a User Account Password 2.1.4 Disable the Guest Account 2.1.5 Lock Out Unwanted Guests 2.1.6 Rename The

		Administrator Account 2.1.7 Disable Jump Lists 2.1.8 Enable Software Updates 2.1.9 Enable Firewall 2.1.10 Adding New Apps In Firewall 2.1.11 Removing/Disabling App Rules From Firewall 2.1.12 Creating a New Firewall Rule 2.1.13 Turn on Windows Defender 2.1.14 Enable bitlocker 2.1.15 Windows Encrypting File System 2.1.16 How to Decrypt a File Using EFS 2.1.17 Disabling Unnecessary Services 2.1.18 Killing Unwanted Processes 2.1.19 How To Hide Files and Folder 2.1.20 Disable Simple File Sharing 2.1.21 Raise The UAC Slide Bar
	2.2 Guidelines To Secure Mac OS X	2.2.1 Lock the System, When Not in Use 2.2.2 Disable Automatic Login 2.2.3 Allow App Downloads from Mac App Store 2.2.4 Enable Automatic Software Updates 2.2.5 Disable Guest Account 2.2.6 Enable FileVault 2.2.7 Enable Firewall 2.2.8 Regularly Change User Account Password 2.2.9 Enable and Set Parental Controls
3. Malware and Antiviruses	3.1 What is Malware	

	3.2 Types Of Malware	3.2.1 Virus 3.2.2 Trojan 3.2.3 Worm 3.2.4 Spyware 3.2.5 Ransomware 3.2.6 Rootkit
	3.3 Symptoms Of Malware Infection	3.3.1 Slow System 3.3.2 Pop Ups 3.3.3 System Crashes 3.3.4 Suspicious Hard Drive Activity 3.3.5 Antivirus Disabling 3.3.6 New Browser Home Page 3.3.7 Peculiar Program Activity
	3.4 Antivirus	3.4.1 What is Antivirus? 3.4.2 How Does Antivirus Work 3.4.3 How Does an Antivirus Deal With an Infected File 3.4.4 How to Choose The Right Antivirus Software 3.4.5 Limitations of Antivirus Software
	3.5 Configuring and Using Antivirus Software	3.5.1 Kaspersky PURE 3.0 3.5.2 Avast Antivirus
	3.6 How To Test If an Antivirus is Working	3.6.1 EICAR Test
4. Internet Security	4.1 Understanding Web Browser Concepts	4.1.1 Internet Security 4.1.2 Introduction to Web Browser 4.1.3 Securing the Web Browser 4.1.4 Browser Features and Their Risks 4.1.5 Identify a Secure Website
	4.2 Understanding IM Security	4.2.1 Instant Messaging (IMing) 4.2.2 Instant Messaging Security Issues

		4.2.3 Instant Messaging Security Measures
	4.3 Understanding Child Online Safety	4.3.1 Risks Involved Online 4.3.2 Determining if Children are at Risk Online 4.3.3 Protecting Children from Online Threats 4.3.4 Encourage Children to Report 4.3.5 How to Report a Crime 4.3.6 Actions To Take When a Child Becomes a Victim of Online Abuse 4.3.7 KidZui
5. Security On Social Networking Sites	5.1 Understanding Social Networking Concepts	5.1.1 Introduction to Virtual Social Networking 5.1.2 Top Social Networking Sites 5.1.3 What is a Profile? 5.1.4 Information Available on Social Networking Sites
	5.2 Understanding Various Social Networking Security Threats	5.2.1 Security Risks Associated with Social Networking Sites 5.2.2 Geotagging 5.2.3 Social Networking Threats to Minors
	5.3 Understanding Facebook Security Settings	5.3.1 Facebook Privacy and Security Settings 5.3.2 Profile Settings 5.3.3 Privacy Settings for Applications 5.3.4 Settings to Block Users 5.3.5 Recommended Actions for Facebook Search Settings 5.3.6 Facebook: Security Tips
	5.4 Understanding Twitter Security Settings	5.4.1 Account Settings 5.4.2 Security Settings 5.4.3 Privacy Settings 5.4.4 Password Settings 5.4.5 Email Notifications 5.4.6 App Settings 5.4.7 Blocking User Accounts

6. Securing Email Communications	6.1 Understanding Email Security Concepts	6.1.1 Introduction to Email 6.1.2 Email Clients 6.1.3 Key Considerations While Choosing an Email Client 6.1.4 Email Service Providers 6.1.5 Email Message 6.1.6 Email Security
	6.2 Understanding Various Email Security Threats	6.2.1 Email Security Threats 6.2.2 Malicious Email Attachments 6.2.3 Malicious User Misdirection 6.2.4 Email Attachments: Caution 6.2.5 Email Security Threats: Phishing 6.2.6 Email Security Threats: Hoax Mail 6.2.7 Nigerian Scam 6.2.8 Email Security Threats: Spamming 6.2.9 Anti-Spamming Tool: SPAMfighter
	6.3 Understanding Various Email Security Procedures	6.3.1 Create and Use Strong Passwords 6.3.2 Disable Keep Me Signed In/Stay Signed In Functions 6.3.3 Provide Recovery Email Address for Mail Recovery 6.3.4 Use HTTPS Enabled Email Service Provider 6.3.5 Turn Off the Preview Feature 6.3.6 Avoid Unwanted Emails Using Filters 6.3.7 Scan Email Attachments for Malware 6.3.8 Check for Last Account Activity 6.3.9 Digitally Sign Your Emails 6.3.10 Encrypt Your Mails

		6.3.11 Email Security Tools
7. Securing Mobile Devices	7.1 Understanding Mobile Device Security Concepts	7.1.1 Securing Mobile Devices 7.1.2 Mobile Device Security 7.1.3 Why Mobile Device Security 7.1.4 Mobile Operating Systems 7.1.5 IMEI Number 7.1.6 Importance of IMEI Number
	7.2 Understanding Threats To a Mobile Device	7.2.1 Mobile Device Security Risks 7.2.2 Mobile Malware 7.2.3 Mobile Application Vulnerabilities 7.2.4 Threats to Bluetooth Devices
	7.3 Understanding Various Mobile Security Procedures	7.3.1 Updating Mobile Operating Systems 7.3.2 Updating Applications in Android Devices 7.3.3 Updating Applications in iOS Devices 7.3.4 Install Mobile Phone Antivirus 7.3.5 Securing Bluetooth Connectivity 7.3.6 Securing Wi-Fi Connectivity 7.3.7 Mobile Device Encryption 7.3.8 Avoiding Mobile Device Theft
	7.4 Understanding How to Secure iPhone and iPad Devices	7.4.1 Securing iPhone and iPad: Enable SIM PIN Protection 7.4.2 Securing iPhone and iPad: Enable Passcode Protection 7.4.3 Securing iPhone and iPad: Enable Touch Id 7.4.4 Securing iPhone and

		iPad: Enable Auto-Lock 7.4.5 Securing iPhone and iPad: iPad Security 7.4.6 Securing iPhone and iPad: Data Backup 7.4.7 Securing iPhone and iPad: Find my iPhone
	7.5 Understanding How to Secure Android Devices	7.5.1 Android: Setting Screen Lock 7.5.2 Android: Setting SIM Lock 7.5.3 Android: Data Backup 7.5.4 Android: Encrypting the Phone 7.5.5 Android: Android Device Manager 7.5.6 Android Data on Your BlackBerry Device
	7.6 Understanding How to Secure Windows Device	7.6.1 Windows: Enabling Password 7.6.2 Windows: Setting up SIM PIN 7.6.3 Windows: Data Backup 7.6.4 Windows: Find My Phone
	7.7 Mobile Security Tools	7.7.1 Lookout Mobile Security 7.7.2 Snap Secure Mobile Security
8. Securing The Cloud	8.1 The Concept of Cloud	8.1.1 Types Of Clouds
		8.1.2 Cloud Services
	8.2 How Cloud Works	8.2.1 Benefits of Cloud
	8.3 Threats To Cloud Security	8.3.1 Data Breach 8.3.2 Data Loss 8.3.3 Account Hacking 8.3.4 Disgruntled Insider 8.3.5 Technology Loopholes 8.3.6 Shared Space
	8.4 Safeguarding Against Cloud Security Threats	8.4.1 Back Up Data 8.4.2 Update Backups Regularly 8.4.3 Create Strong Passwords 8.4.4 Choose Two Step

		Authentication 8.4.5 Encrypt 8.4.6 Have a Disciplined Online Behavior 8.4.7 Avoid Storing Sensitive Data on Cloud
	8.5 Cloud Privacy Issues	8.5.1 Data Ownership 8.5.2 Data Location 8.5.3 Data Migration 8.5.4 Data Permanency
	8.6 Addressing Cloud Privacy Issues	8.6.1 Encrypt 8.6.2 Read Terms and Conditions Carefully 8.6.3 Avoid the Share Feature on Cloud 8.6.4 Avoid Storing Sensitive Data on Cloud
	8.7 Choosing a Cloud Service Provider	8.7.1 Questions to Ask Before Choosing a Service Provider
9. Securing Network Connections	9.1 Understanding Various Networking Concepts	9.1.1 Types of networks 9.1.2 Recognize the options for connecting to a network like: cable, wireless. 9.1.3 Home Network 9.1.4 Steps for Home Networking 9.1.5 Wireless Networks
	9.2 Understanding Setting Up a Wireless Network in Windows	9.2.1 Setting Up a Wireless Network in Windows
	9.3 Understanding Setting Up a Wireless Network in Mac	9.3.1 Setting Up a Wireless Network in Mac
	9.4 Understanding Threats to Wireless Network Security and Countermeasures	9.4.1 Common Threats to Wireless Network 9.4.2 Securing Wireless Network
	9.5 Measures to Secure Network Connections	9.5.1 Use Firewall 9.5.2 Use Antivirus 9.5.3 Use Encryption
10. Data Backup and Disaster	10.1 Data Backup Concepts	10.1.1 Data Backup

Recovery		10.1.2 Need for a Data Backup
		10.1.3 Reasons for Data Loss
		10.1.4 What Files to Backup and How Often
	10.2 Types of Data Backups	10.2.1 Full Backup
		10.2.2 Incremental Backup
		10.2.3 Differential Backup
		10.2.4 Online Data Backup
	10.3 Windows Backup and Restore Procedures	10.3.1 Full Backup in Windows
		10.3.2 Incremental Backup in Windows
		10.3.3 Restoring Backed Up Data
	10.4 MAC OS X Backup and Restore Procedures	10.4.1 Time Machine (Apple Software)
		10.4.2 Setting Up Time Machine
		10.4.3 Restoring Files from Time Machine Backups
	10.5 Understanding Secure Data Destruction	10.5.1 Why Do We Need to Destroy Data Permanently?
		10.5.2 Deletion Vs. Permanent Destruction
		10.5.3 Ways to Permanently Destroying Data