Certified Secure Computer User

Course Description

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

Who Should Attend

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

Course Outline

Module 01: Foundations of Security

- Essential Terminologies
- Computer Security
- Why Security?
- Potential Losses Due to Security Attacks
- Elements of Security
- The Security, Functionality, and Ease of Use Triangle
- Fundamental Concepts of Security
- Layers of Security
- Security Risk to Home Users
- What to Secure?
- What Makes a Home Computer Vulnerable?
- What makes a System Secure?
- Benefits of Computer Security Awareness
- Basic Computer Security Checklist

Module 02: Securing Operating Systems

- System Security
- Threats to System Security
    - Password Cracking
- Guidelines for Windows OS Security
    - Lock the System When Not in Use
    - Create a Strong User Password
    - Change Windows User Password: Windows 7
    - Disable the Guest Account: Windows 7
    - Lock Out Unwanted Guests in Windows 7
    - Rename the Administrator Account in Windows 7
    - Disable Start up Menu in Windows 7
    - Windows Updates in Windows 7
    - Pointers for Updates
    - Apply Software Security Patches
    - Configuring Windows Firewall in Windows 7
    - Adding New Programs in Windows Firewall in Windows 7
    - Removing/Disabling Programs Rules from the Windows Firewall in Windows 7
    - Creating a New Windows Firewall Rule in Windows 7
    - Two-Way Firewall Protection in Windows
    - Always Use NTFS
- Windows Encrypting File System (EFS)
    - How to Decrypt a File Using EFS in Windows?
- Using Windows Defender
- Enable BitLocker in Windows 7
- Launching Event Viewer in Windows 7
    - Event Viewer: Events and How to Read Logs on the System
- Disabling Unnecessary Services in Windows 7
- Killing Unwanted Processes
- Finding Open Ports Using Netstat Tool

- Configuring Audit Policy
- How to Hide Files and Folders?
- Disable Simple File Sharing in Windows
- Raise the UAC Slider Bar in Windows 7
- Windows Security Tools
    - Windows Security Tools: Microsoft Security Essentials
    - Windows Security Tools: KeePass Password Safe Portable
    - Windows Security Tools: Registry Mechanic
- Guidelines for Securing Mac OS X
    - Step 1: Enabling and Locking Down the Login Window
    - Step 2: Configuring Accounts Preferences
    - Step 3: Guidelines for Creating Accounts
    - Step 4: Securing the Guest Account
    - Step 5: Controlling Local Accounts with Parental Controls
    - Step 6: Use Keychain Settings
    - Step 7: Use Apple Software Update
    - Step 8: Securing Date & Time Preferences
    - Step 9: Securing Network Preferences
    - Step 10: Enable Screen Saver Password
    - Step 11: Set Up FileVault to Keep Home Folder Secure
    - Step 12: Firewall Security
- Operating Systems Security Checklist
- Security Checklist for Windows 7
- MAC OS Security Checklist

Module 03: Protecting System Using Antiviruses

- Introduction to Antivirus Software
- Need for Antivirus Program
- How Does Antivirus Software Work?
- Antivirus Software 2011
- Choosing the Best Antivirus Software

- Steps to Install Antivirus on Your Computer
- How to Test If Antivirus Is Working
- Configuring McAfee Antivirus
- Configuring Kaspersky PURE
- Antivirus Security Checklist

Module 04: Data Encryption

- Common Terminologies
- What is Encryption?
- Objectives of Encryption
- Usage of Encryption
- Types of Encryption
    - Symmetric vs. Asymmetric Encryption
- Encryption Standards
- Digital Certificates
- How Digital Certificates Work?
- Digital Signature
- Cryptography Tools

Module 05: Data Backup and Disaster Recovery

- Data Backup
- Need for Backup
- Types of Data Loss
- What Files to Backup and How Often?
- Online Data Backup
- Online Backup Service Providers
- Types of Backup
- Back Up the Data Using Windows Backup
    - Steps to Backup Data
    - Restoring Data
- Securing Backup on Storage Devices with Encryption

- Time Machine (Apple Software)
    - Setting Up Time Machine
    - Restoring Files from Time Machine Backups
- Data Backup Tools for Windows
    - Acronis True Image Home 2011
    - NovaBACKUP Home Protection
    - Data Backup Tools for Windows
- Data Backup Tools for MAC OS X
    - MAC OS X Data Backup Tool: Data Backup
    - MAC OS X Data Backup Tool: SmartBackup
    - Data Backup Tools for MAC OS X
- Data Recovery Tools for Windows
    - Windows Data Recovery Tool: Recover My Files
    - Windows Data Recovery Tool: EASEUS Data Recovery Wizard
    - Data Recovery Tools for Windows
- MAC OS X Data Recovery Tool
    - Boomerang Data Recovery Software
    - VirtualLab
    - Data Recovery Tools for MAC OS X
- Physical Security
    - Physical Security Measures: Locks
    - Physical Security Measures: Biometrics
    - Physical Security Measures: Fire Prevention
    - Physical Security Measures: HVAC Considerations
    - Securing Laptops from Theft
    - Laptop Theft Countermeasures
- Data Backup Checklist
- Physical Security Checklist

Module 06: Internet Security

- Internet Security

- Internet Explorer Security Settings
    - Internet Explorer Security Settings: Internet Zone
    - Internet Explorer Security Settings: ActiveX Controls
    - Internet Explorer Security Settings: Local Intranet Zone
    - Internet Explorer Security Settings: Trusted Sites Zone
    - Internet Explorer Security Settings: Restricted Zone
- Understanding Cookies
- Internet Explorer Privacy Settings
    - Deleting Browsing History
    - Do Not Allow the Browser to Remember any Password
- Securing File Downloads
- Mozilla Firefox Security Settings
- Mozilla Firefox: Privacy Settings
- Securing File Downloads
- Installing Plugins
- Google Chrome Privacy and Security Settings
    - Google Chrome: Privacy Settings
    - Google Chrome: Security Settings
- Apple Safari Security Settings
- Testing the Browser for Privacy
- Instant Messaging (IMing)
    - Instant Messaging Security Issues
    - Instant Messaging Security Measures
- Searching the Web
- Online Gaming and MMORPG
    - Online Gaming Risks
    - Insecure or Compromised Game Servers and Game Coding
    - Social Risks
    - Social Engineering
- Protection Schemes, Cyber Prostitution, and Virtual Mugging
- How the Malicious Users Make Money?

- Security Practices Specific to Gaming
    - Recognize Administrator Mode Risks
    - Recognize Risks due to ActiveX and JavaScript
    - Play the Game, Only at the Game Site
    - Pay Attention to Firewall Management
- Child Online Safety
    - Risks Involved Online
        - Misdirected Searches
        - Stealth Sites and Misleading URLs
        - Child Pornography, Grooming, and Cyberbullying
- Role of Internet in Child Pornography
    - Effects of Pornography on Children
    - Risks Involved in Social Networking Websites
- Unsolicited Emails
- Chat Rooms
- Finding if Children are at Risk Online
- Protecting Children from Online Threats
- Encourage Children to Report
- How to Report a Crime?
- Security Software Checklist
    - KidZui
- Actions to Take When the Child Becomes an Online Victim
- Internet laws
- Laws Internet users should know
    - USA PATRIOT Act
    - Children's Online Privacy Protection Act (COPPA)
    - The Digital Millennium Copyright Act
        - Highlights of DMCA
    - CAN-SPAM Act
    - Computer Misuse Act 1990
    - European Union Data Protection Directive (95/46/EC)

- Data Protection Act 1998
- Internet Security Checklist
- Guidelines for Parents to Protect Children from Online Threats

Module 07: Securing Network Connections

- Home Network
  - Network Devices
  - Steps for Home Networking
- Wireless Networks
  - Setting Up a Wireless Network in Windows 7
    - Changing Wireless Networking Configuration in Windows 7
  - Setting Up a Wireless Network in Mac
    - Changing Wireless Networking Configuration in Mac
- Common Threats to Wireless Network
- Securing Wireless Network
- Using the Network with Windows 7
  - Setting Up the PC's Name and Workgroup Name in Windows 7
  - Sharing
  - Transferring Files
  - Simple File Sharing in Windows 7
  - Hiding a Shared Disk or Folder
  - How to Share Printer in Windows 7?
  - Using Printers on Other PC's
  - Accessing Files on Other PCs
  - Windows Easy Transfer
- Using the Network with MAC OS X
  - Setting Up the PC's Name in MAC OS X
  - Setting Up the Workgroup Name in MAC OS X
  - Creating User Accounts and Groups in MAC OS X
  - Sharing Files and Folders in Macintosh OS X
  - Printer Sharing in Macintosh OS X

- Accessing Other Macs on Your Network
- Network Security Threats
- Securing Network Connections
  - Use Firewall
  - Use Antivirus Protection
  - Use Strong Passwords, Make Regular Backups, and Know about Encryption
  - Identify a Secure Website
- General Security Practices in Home Networking
- Network Adapters
  - Checking Network Adapter
  - Network Setup Wizard
  - How to Isolate Networking Problems (Windows 7): Network Adapter?
  - Network Adapter Status
- Troubleshooting with Network Adapters
  - Network Adapter is Unplugged
  - Network Adapter Has Limited or No Connectivity
  - Network Adapter is Connected, but User Cannot Reach the Internet
- Network Security Checklist

Module 08: Securing Online Transactions

- Online Shopping
  - How Online Shopping Works?
- Online Banking
- Credit Cards Payments
- Types of Credit Card Frauds
- Guidelines for Ensuring Credit Card Safety
- Securing Online Transactions
- Online Payment Services
  - Choosing a Secure Online Payment Service
- SSL and the Padlock Symbol
  - What Does the SSL Show?

- Identifying a Trustworthy Website
- Identifying an Untrustworthy Website
- McAfee's Site Advisor
    - Rating Icons
- Online Transactions Security Checklist

Module 09: Securing Email Communications

- Email Security
- Email Security Threats
    - Malicious Email Attachments
        - Email Attachments: Caution
    - Spamming
        - Spamming Countermeasures
            - Anti-Spamming Tool
    - Hoax/Chain Emails
    - Scam Emails
        - Nigerian Scam
- Email Security Procedures
    - Creating Strong Passwords
    - Alternate Email Address
    - Keep Me Signed In/Remember Me
    - Using HTTPS
    - Check for Last Account Activity
    - Scanning Email Attachments
    - Turn Off Preview Feature
    - Email Filtering: Avoiding Unwanted Emails
    - Digitally Sign Your Emails
        - How to Obtain Digital Certificates?
        - Installing Digital Certificate
        - Signing your Emails
    - Microsoft Outlook Download Settings

- Online Email Encryption Service
- Email Security Tools
- Email Communication Checklist
- Email Security Checklist
- Security Checklist for Checking Emails on Mobile

Module 10: Social Engineering and Identity Theft

- What Is Identity Theft?
    - Personal Information that Can be Stolen
    - How Do Attackers Steal Identity?
    - What Do Attackers Do with Stolen Identity?
    - Identity Theft Example
- Social Engineering
    - Social Engineering Examples
    - Human-Based Social Engineering
    - Computer-Based Social Engineering
        - Computer-Based Social Engineering: Phishing
        - Phony Security Alerts
    - Computer-based Social Engineering Through Social Networking Websites
- How to Learn if You Are a Victim of Identity Theft
- What to Do if Identity Is Stolen
- Reporting Identity Theft
    - Federal Trade Commission
    - econsumer.gov
    - Internet Crime Complaint Center
- Prosecuting Identity Theft
- Protecting from Identity Theft
    - IP Address Hiding Tools
- Identity Theft Protection Checklist
- Computer Based Identity Theft Protection Checklist

Module 11: Security on Social Networking Sites

- Social Networking Sites
- What Is a Profile?
- Top Social Networking Sites
- Security Risks Involved in Social Networking Sites
    - Cyberbullying
    - Identity Theft
    - Phishing Scams
    - Malware Attacks
    - Site Flaws
- Social Networking Threats to Minors
- Facebook Privacy Settings
    - Profile Settings
    - Privacy Settings for Applications
    - Settings to Block Users
    - Recommended Actions for Facebook Search Settings
    - Facebook: Security Tips
- Staying Safe on MySpace
- Social Networking Security Checklist
- Social Networking Security Checklist for Parents and Teachers

Module 12: Information Security and Legal Compliance

- HIPPA
    - HIPPA Checklist
- FERPA
    - FERPA Checklist
- PCI DSS
    - PCI DSS Checklist

Module 13: Securing Mobile Devices

- Mobile Device Security

- Mobile Phone Services
- IMEI Number
- Mobile Device Security Risks
    - Mobile Malware
    - Mobile Application Vulnerabilities
- Threats to Bluetooth Devices
- Mobile Security Procedures
    - Patching Mobile Platforms and Applications
    - Avoid Mobile Device Theft
    - What to DO if Your Mobile is Lost or Stolen
    - Use Power-On Authentication
    - Regularly Back Up Important Data
    - Use Encryption to Secure Data in Mobile Device
    - Enable the Auto-Lock Feature
    - Install Only Signed Applications
    - Install Mobile Phone Anti-Virus
    - Mobile Phone Anti-Virus Tools
    - Secure Bluetooth Connectivity
- Securing iPhone and iPad
    - Enable Passcode Protection
    - Enable SIM PIN Protection
    - Enable Auto-Lock and Re-map Button
    - iPad Security
- Securing Blackberry and Windows Phone 7 Mobiles
    - BlackBerry: Setting Device Password
    - BlackBerry: Changing the Device Password
    - BlackBerry: Lock Your Device
    - BlackBerry: Device Password
    - BlackBerry Password Keeper
    - Encrypting Data on Your BlackBerry Device
    - Windows Phone 7 Mobiles: Use of PIN to Lock SIM Card

- Windows Phone 7 Mobiles: Changing the Password of the Phone

- Mobile Security Tools
- Bluetooth Security Checklist
- Mobile Phone Security Checklist