awantec ROCHESTON

Enhance human potential through life-long learning

Audience Profile

- Any individual, organization, government agency, from school students to homemakers
- Technically and non-technically inclined people
- Everyday users of digital technology

Course Objectives

- Gain credible recognition as a Cybersecurity Specialist
- Best practices in fundamentals of cybersecurity
- Better control over your own devices and data
- Better privacy and security of personal information
- Best strategies to ensure secure payments on e-platforms
- Secure social media usage

Course Duration

2 Days

Rocheston Certified Cybersecurity Specialist (RCCS)

Course Description

Rocheston Certified Cybersecurity Specialist (RCCS) will provide the learners with a working knowledge of all the fundamental threats to cybersecurity in our everyday life and how to deal with them. Every end user, that is, almost every single one of us in today's world, who has a minimum digital footprint, needs to be educated in the ways to secure their devices and systems. The course is designed for ordinary day-to-day users who do not have the advantage of specialized technical knowledge to gain a solid foundation in cybersecurity.

Course Outline

Module 1: Securing Data and Privacy

- Macro and Micro Impact of Privacy Breach
- Policy Development and Privacy Management
- How to block a number on iOS and Android
- Setting up VPN for a smart TV
- Sharing VPN on Windows and OS X
- Going Incognito
- Securing online bank transactions

Module 2: How to Avoid Getting Scammed Online

- What are scams?
- What is online fraud?
- Types of Online Scams
- What to Keep in Mind to Avoid Getting Scammed
- How to Spot Online Fraud/Scam
- How to Prevent Getting Scammed
- What is Spoofing
- Internal social engineering
- Internal online fraud protection
- Phishing protection
- Malicious antivirus identification
- Malware protection
- Malicious software scenario policies
- Verification standards for information seekers

Course Outline

Module 3: Securing Networks

- Securing Organizational Networks
- Securing Passwords
- Securing the Network
- Securing Wi-Fi
- Securing sensitive data
- Updates and patches
- Internal update practices
- Third party app update practices
- Update rollout
- Securing browsing
- Securing files
- File upload and sharing practices
- Securing remote access

Module 4: Securing Websites

- Authentication and cryptography
- Potential threats
- How to secure websites
- Securing public web servers
- Training and development for web security
- Security management practices
- Standardized software configurations
- Server configuration
- Securing web server operations
- Securing Web Server Application
- Securing content

Module 5: Securing Emails

- Email security
- Email encryption
- Spam filter practices
- Responsible internal email usage
- Sensitive information sharing practices
- Retention policy
- Email usage policy

Module 6: Securing Mobile Devices

- Vulnerabilities in smartphone devices
- Cyber threats to mobile devices
- Best practices for securing mobile devices
- Software security
- Effective mobile device management
- What to do if mobile device is stolen or lost

Module 7: Securing Employees

- Background check policy in recruitment
- Background check policy for vendor and partners
- Access control
- What is a Human Firewall?
- Training employees in cybersecurity
- Sensitive information

Module 8: Securing Operations

- Security policy
- Identifying critical information
- Analyzing information
- Analyzing vulnerabilities
- Identifying potential exploitations
- Other steps to successfully implement OPSEC

Module 9: Securing Payments

- Securing customer payment
- Data storage policy
- Security tools and resources
- Access controls
- Security basics

awantec

Awantec Systems Sdn. Bhd. Reg. No. 200301028384 (630804-K)
(Formerly known as Prestariang Systems Sdn. Bhd.)

Block 11B, Star Central,
Lingkaran Cyber Point Timur, Cyber 12,
63000 Cyberjaya, Selangor, Malaysia.

+6 03 8689 7000
learning@awantec.my
www.awantec.com.my

Course Outline

Module 10: Incident Response and Reporting: A Guideline

- What is an incident?
- Types of breaches
- Physical breaches
- Network breaches
- Data breaches
- Incidence response
- Reporting an incident

Module 11: Social Media: Policy Development and Management

- Security roles and responsibilities
- Internal internet usage
- Social media policy

Module 12: Cybersecurity Basics

- Anti-virus software
- Application
- Authentication
- Authorization
- Backdoor
- Backup
- Bandwidth

Module 13: Cybersecurity Basics

- Blacklisting software
- Brute Force Attack
- Clear Desk Policy
- Clear Screen Policy
- Cookie
- Cyberbullying
- Cybersecurity
- Cyber threats
- Denial of Service Attack
- Dictionary Attack
- Digital Certificate
- Domain Hijacking
- Domain Name System (DNS)
- Dumpster Diving
- Electronic Infections
- Encryption
- End User License Agreement (EULA)
- File-Sharing Programs
- Firewall
- Flooding
- Grooming
- Hacker
- HTTPS
- Firewall
- Flooding
- Grooming
- Hacking
- HTTPS
- Hybrid Attack
- Instant Messaging (IM)
- IP (Internet Protocol) Address
- Internet Service Provider (ISP)
- Keystroke Logger
- Malware
- Man-In-the-Middle Attack
- Monitoring software
- Network
- Operating System (OS)
- Password
- Password Cracking
- Password Sniffing
- Patch
- Peer-to-Peer (P2P) Programs
- Phishing
- Router
- Script
- Shoulder Surfing
- Skimming
- Sniffing
- Social Engineering