Cyber Specialist

Exam CPCS-100

Domain 1: Introduction to Cybersecurity & Digital Safety

1.1 : Define cybersecurity, explain its importance in today's world, and describe key cybersecurity terminology.

1.2 : Identify common cyber threats (e.g., malware, phishing, ransomware).

1.3 : Describe safe internet browsing habits and how to recognize scams.

1.4 : Explain the importance of strong passwords and multi-factor authentication.

1.5 : Understand the impact of cyber threats on individuals, businesses, and society.

Domain 2: Cybersecurity Laws, Ethics, and Government Agencies

2.1 : Identify major cybersecurity laws and regulations (e.g., GDPR, CIPA, COPPA).

2.2 : Understand the role of government agencies in cybersecurity (e.g., NSA, CISA, FBI).

2.3 : Discuss ethical dilemmas in cybersecurity (e.g., hacking, digital privacy).

2.4 : Explain how cybersecurity policies, including internal policies and compliance frameworks, protect businesses and consumers, and discuss the role of health, safety, and environmental management in compliance.

2.5 : Understand the consequences of cybercrimes and their legal impact.

Domain 3: Cyber Threats & Attack Methods

3.1 : Identify different types of cyberattacks (e.g., DDoS, man-in-the-middle, ransomware).

3.2 : Explain how hackers exploit system vulnerabilities.

3.3 : Understand how artificial intelligence (AI) is used in cyberattacks and defense, including automated threat detection, machine learning-based security analytics, and AI-driven cyber defense.

3.4 : Describe the motivations behind cyberattacks (e.g., financial gain, espionage).

3.5 : Discuss the role of ethical hackers in preventing cyber threats and explain intrusion methods, attacker motivations, and hacking techniques.

Domain 4: Cybersecurity Tools & Defensive Technologies

4.1 : Explain how antivirus software and firewalls protect systems.

4.2 : Describe how Intrusion Detection Systems (IDS) monitor network security.

4.3 : Compare host-based and network-based IDS technologies.

4.4 : Explain how Virtual Private Networks (VPNs) enhance security.

4.5 : Understand how cloud computing and virtualization are secured and protected from cyber threats, including the use of open-source security tools, container security, and hypervisor vulnerabilities.

Domain 5: Cryptography & Data Protection

5.1 : Define encryption and explain its role in cybersecurity.

5.2 : Identify common cryptographic algorithms (e.g., AES, RSA).

5.3 : Understand how digital signatures verify authenticity.

5.4 : Explain Public Key Infrastructure (PKI), including the role of digital certificates in authentication, encryption, and secure communication.

5.5 : Explore steganography and its use in cybersecurity.

Domain 6: Cybersecurity Risk Management & Incident Response

6.1 : Define risk management and explain how businesses assess cybersecurity risks.

6.2 : Understand how organizations create cybersecurity policies and procedures.

6.3 : Learn about incident response plans and how companies react to cyberattacks.

6.4 : Discuss the role of penetration testing in cybersecurity defense, including penetration testing methodologies and tools (e.g., Kali Linux, Metasploit, vulnerability scanners).

Domain 7: Securing Devices, Networks, and Virtual Environments

7.1 : Describe how to secure personal devices (e.g., computers, smartphones).

7.2 : Explain best practices for securing Wi-Fi networks.

7.3 : Understand vulnerabilities unique to virtual environments.

7.4 : Describe the importance of securing IoT (Internet of Things) devices by identifying common vulnerabilities, implementing device authentication, and using network segmentation to limit security risks.

7.5 : Explore emerging cybersecurity challenges in cloud computing.

Domain 8: Social Engineering & Human Factors in Cybersecurity

8.1 : Define social engineering and describe common scams.

8.2 : Explain how attackers use manipulation to steal personal information.

8.3 : Identify ways to recognize and prevent phishing attacks.

8.4 : Discuss how businesses train employees to avoid cyber threats.

8.5 : Understand the risks of oversharing personal information online.

Domain 9: Cybersecurity Careers & Industry Pathways

9.1 : Explore different careers in cybersecurity (e.g., ethical hacker, forensic analyst).

9.2 : Identify cybersecurity certifications and discuss the skills and education needed for a career in cybersecurity.

9.3 : Understand the importance of hands-on experience in cybersecurity through labs, certifications, and industry-recognized challenges.

9.4 : Develop essential soft skills (e.g., teamwork, leadership, problem-solving) to succeed in cybersecurity careers.

Domain 10: Cybersecurity for Business & Entrepreneurship

9.1 : Explain why cybersecurity is important for small businesses.

9.2 : Discuss cybersecurity risks that businesses face (e.g., data breaches, fraud).

9.3 : Explore business opportunities in the cybersecurity industry.

9.4 : Identify ways businesses can protect customer data.

9.5 : Learn how to create a cybersecurity business plan or startup idea.