# Course Planning Template

| | |
|---|---|
| **Course Title** | Foundations of Cyber Security |
| **Course Length** | 6 weeks, with 11 lectures of 2 hours each. |
| **Target Audience** | This course is designed for:<br>• Anyone interested in **understanding cyber security basics** for personal or professional purposes, including homemakers, seniors, students, and non-tech professionals.<br>• Small business owners and home office individuals **needing to secure their digital assets and data**.<br>• Individuals considering a career in cyber security and **looking to understand the fundamentals**.<br>• Computer science students or IT professionals wishing to **broaden their cyber security knowledge**. |
| **Language of Instruction** | Bilingual - English and Urdu |

| **Course Description** |
|---|
| This course, "Cyber Security Foundation", offers a comprehensive introduction to the exciting and ever-evolving field of cybersecurity. Accessible to individuals from all backgrounds and levels of technological proficiency, this course aims to demystify the subject, making cybersecurity understandable and applicable to everyone. Through this course, participants will familiarise themselves with the basic principles of cyber security, the different types of threats and attacks in the digital world, and how they can defend against them using various security technologies. We will explore crucial topics such as social engineering, cryptography, malware, digital forensics, and risk management. Furthermore, the course will explore how cyber security can be improved at an organisational or personal level and how a cyber security culture can be cultivated. The course wraps up with a look into the future directions of cyber security. |

| Course Learning Outcomes | |
|---|---|
| | By the end of this course, the students should be able to: |
| LO1: | Understand the fundamental concepts and importance of cyber security, including different types of cyber threats, attacks, and the basic principles of cryptography. |
| LO2: | Identify various social engineering tactics and malware types, and apply preventive measures and mitigations to protect against these threats. |
| LO3: | Assess the cyber security posture of an organisation or home, apply various security technologies, and understand the importance and implementation of a robust cyber security policy. |
| LO4: | Understand and implement principles of risk management, incident response, disaster recovery, and business continuity in the context of cyber security. |
| LO5: | Recognise and discuss emerging trends and future directions in cyber security, and understand the significance of cultivating a cyber security culture. |

| Assessments/Graded Components |
|---|
| **Attendance and Participation:** Regular attendance is required for this course and will contribute to the completion certificate. This includes active involvement in class discussions, hands-on activities, and interactive exercises. |

**Course Summary**

| Lecture | Module Name | Key Concepts/Topics Covered | Assessments |
|---|---|---|---|
| 1 | Introduction to Cyber Security | Importance of Cyber Security, Real-World Attacks, Basic Concepts and Goals (CIA), Overview of Cyber Threats, Eavesdropping, Alterations, Denial of Service, Masquerading, Repudiation, Correlations and Traceback | |

| | | | |
|---|---|---|---|
| 2 | Social Engineering | Definition, Types (Phishing, Vishing, Tailgating, Dumpster Diving, Shoulder Surfing, Eavesdropping), Public Hotspot Attacks, QR code Attacks | |
| 3 | Cryptography | Cryptography vs Steganography, Classical Ciphers, Cryptoanalysis, Symmetric and Asymmetric Cryptography, Hash Functions, Digital Signatures | |
| 4 | Malware and Privacy | Types of Malware, Malware Life Cycle, Privacy Concepts, Policies, Issues, and Anonymity | |
| 5 | Security Technologies | Principles of Security, Firewall, Intrusion Prevention and Detection Systems, Pentesting, VPN, SSL/TLS, Certificates, Blockchain | |
| 6 | Digital Forensics | Introduction to Digital Forensics, History, Standards, Fundamentals of Digital Forensic Investigations | |
| 7 | Cyber Security Posture Assessment | Pillars of Security Management, Information Security Management System (ISMS), Risk Management, Self-assessment Techniques | |
| 8 | Crafting a Cyber Security Policy | Importance and Design Cycle of a Cyber Security Policy, Policy Benchmarks, Example Policies | |
| 9 | Risk Management and Incident Handling | Definition of Risk, Risk Management Process, Incident Response, Disaster Recovery, Business Continuity, Physical Security | |
| 10 | Emerging Trends in CyberSecurity | Internet of Things (IoT) Security, Drone Security | |