

CYBER SECURITY ESSENTIALS

Course Code: CSC 201

Credit Units: 03

Total Hours: 30

Course Objectives:

- Understand the field of digital security and concepts of access control mechanism.
- To introduce keywords and jargons involved in securing browser
- Understanding network basic and familiarize on security of network protocols
- Awareness and understanding on cyber-attacks and data privacy.

Course Contents:

Module I: Digital Security Primitives: (8 hours)

Basics of digital security, protecting personal computers and devices, protecting devices from Virus and Malware, Identity, Authentication and Authorization, need for strong credentials, keeping credentials secure, protecting servers using physical and logical security, World Wide Web (www), the Internet and the HTTP protocol, security of browser to web server interaction.

Module II: Networking basics: (6 hours) Design of secured networks, security for SOHO, designing home networks and VPN, managing DMZ, home network and large-scale business networks, Networking protocols, Security of protocols, sample application hosted on-premises, Information Destroying and Recovery Tools, Recovering from Information Loss, Destroying Sensitive Information.

Module III: Detection and Prevention of cyber-attacks: (8 hours)

Introduction to cyber-attacks, application security (design, development and testing), operations security, monitoring, identifying threats and remediating them, Principles of data security - Confidentiality, Integrity and Availability, Data Privacy, Data breaches, preventing attacks and breaches with security controls, Compliance standards, Computer Ethics.

Module IV: Architecture of Security System: (8 hours)

Security Architecture - an overview, Fundamentals of Designing Secure Computer Systems, Security Architecture and Design, Purpose of Cybersecurity Architecture, scopes of security architecture and paradigm, basics of ethical hacking and penetration testing.

Course Outcomes:

The student will learn

- Apply a solid foundation in digital security and measures taken to protect device from threats.
- Learning access control mechanism and understand how to protect servers

- Understand the importance of a network basics and brief introduction on security of network protocols
- To understand cyber-attacks and learn data privacy issues and preventive measures.

Examination Scheme:

Components	A	CT	S/V/Q/HA	EE
Weightage (%)	5	15	10	70

A: Attendance, CT: Class Test, S/V/Q/HA: Seminar/Viva/Quiz/ Home Assignment, EE: End Semester Examination.

Text & References:

- Sammons, John, and Michael Cross. The basics of cyber safety: computer and mobile device safety made easy. Elsevier, 2016.
- Charles P. Pfleeger, Shari Lawrence, Pfleeger Jonathan Margulies; Security in Computing, Pearson Education Inc . 5th Edition, 2015
- Brooks, Charles J., Christopher Grow, Philip Craig, and Donald Short.; Cybersecurity essentials. John Wiley & Sons, 2018