Seminar Topic Summary Report

Tentative Cover Page

Institution Name: Basaveshwar Engineering College, Bagalkot

Department of Computer Applications (M C A)

Course: MCA

Semester: II

Seminar Topic : cyber security challenges

Submitted by: Shrishail biradar

USN: 2BA24MC037

Student Name: Shrishail biradar

Date of Submission:26-06-2025

Guide/Faculty Name: Prof. C.M Jangin

Guide Signature:

Tentative Index Page

Table of Content

1. Introduction

In the rapidly evolving digital world, Cyber Security has emerged as a critical area of concern. With the growing dependence on internet-based technologies, safeguarding sensitive data and ensuring the integrity of systems has become more important than ever. Cyber Security refers to the practice of protecting computers, networks, programs, and data from unauthorized access, attacks, and damage. The rise in cybercrimes such as phishing, hacking, ransomware, and identity theft poses serious threats to individuals, organizations, and governments. For students of Computer Applications, understanding Cyber Security is essential not only for academic growth but also for building a secure digital future. This seminar aims to explore the fundamentals, threats, and defense mechanisms in cyber security, helping students develop awareness and readiness to handle real-world security challenges.

1. Digital Era & Data Importance
2. Increased Use of Technology
3. What is Cyber Security
4. Types of Cyber Threats
5. Why Cyber Security is Import
6. Cyber Crime is Growin
7. Relevance for MCA Student
8. Objective of the Seminar
9. Career Significance

2. Seminar Topic Details

*Title of the Topic:

Cyber Security Challenges

*Area/Domain:
cyber security / Information Security

* Keywords:

*Cyber Threats – Unauthorized attempts to access or damage systems and data

*Network Security – Protection of computer networks from intrusions and misuse

*Data Breach – Unauthorized access and disclosure of confidential information

*Malware & Ransomware – Malicious software used to damage, steal, or lock data

*Phishing Attacks – Fraudulent communication aimed at stealing sensitive data Zero-Day

Vulnerabilities

*Unknown flaws exploited before they are patched

*Digital Privacy – Protecting personal and organizational data from exposure

*Ethical Hacking – Testing systems for vulnerabilities to improve security

*Cloud Security – Securing data and systems hosted on cloud platforms

*Cyber Law & Compliance – Legal and ethical standards for cyber protection

*Brief-Description:
This seminar focuses on the major challenges faced in the field of cyber security today, such as evolving malware, increased ransomware attacks, lack of user awareness, and gaps in system security. It highlights both technical and human-related risks, explores real-world case studies, and presents solutions like encryption, firewalls, intrusion detection systems, and awareness training. Emphasis will be given to how professionals and students can stay ahead of cybercriminals using updated tools, secure practices, and global security standards.

3. Topic Summary

Cyber Security refers to the set of practices and technologies designed to protect digital information and systems from cyberattacks, unauthorized access, or data breaches. As businesses and individuals increasingly rely on digital platforms, the risk of cyber threats like malware, ransomware, phishing, and denial-of-service (DoS) attacks has escalated. These attacks can lead to financial losses, reputational damage, and serious data compromise.

The topic of cyber security encompasses several domains:

- Network Security: Preventing unauthorized access or misuse of networks.
- Application Security: Securing software and devices from vulnerabilities.
- Information Security: Protecting data from unauthorized access and modification.
- Operational Security: Managing and protecting data handling procedures.
- Disaster Recovery & Business Continuity: Planning for recovery after an attack.
- End-user Education: Training users to follow good security practices.

Recent trends include the integration of Artificial Intelligence in cyber defense, Zero Trust Architecture, cloud security, and ethical hacking as a proactive measure. As cyber threats evolve, so do the defense strategies, making it a dynamic and highly significant area of study.

4. Relevance to MCA Curriculum

: The topic "Cyber Security Challenges" is highly relevant to the Master of Computer Applications (MCA) curriculum, as it directly aligns with both theoretical and practical components of the program. In today’s digital world, securing data, systems, and applications has become a core requirement for all IT professionals, making cybersecurity an essential area . subject: computer network, information security, operating system

Key Connections to the MCA Curriculum:

1. Related Subjects:
   - o Computer Networks – Understanding data transmission and network security principles.
2. gain practical skills in identifying threats, designing secure systems, and responding to incidents.
   - o Encourages the implementation of secure coding practices and system hardening techniques.
3. Professional Readiness:
   - o Prepares audience roles such as Cyber Security Analyst, Ethical Hacker, Penetration Tester, or Security Consul
4. Project & Internship Alignment:
   - o Cybersecurity projects and internships allow students to apply their knowledge in practical environments, such as conducting vulnerability assessments or designing secure apps.

5 Objectives : By attending this seminar, will be able to:

- Understand the fundamentals of Cyber Security, its key concepts, and importance in the digital world.
- Analyze the major challenges faced in securing networks, systems, and applications, especially in modern IT environments like cloud and. Learning IoT.
- Explore current technologies and strategies used to defend against cyberattacks, such as encryption, firewalls, intrusion detection systems, and multi-factor authentication.
- Gain awareness of ethical, legal, and regulatory aspects of cyber security, including data protection laws like GDPR and the Indian IT Act.

6. Expected Outcome: By the end of the seminar, participants are expected to:

- Gain a clear understanding of current cyber security threats and challenges affecting individuals, organizations, and governments. Develop the ability to analyse and respond to various cyber threats using appropriate tools and techniques. Enhance awareness of best practices in cyber hygiene and secure system design, which are essential for safe digital interaction. Understand the importance of compliance with cyber laws and data protection regulations, and how these affect software and system development.

7. References

* William Stallings, Network Security Essentials: Applications and Standards, Pearson, 2017.

* Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing, Pearson, 2015.

Coordinator Signature: HOD Signature: