**Seminar Topic Summary Report**

**Institution Name: Basaveshwar Engineering College, Bagalkot**

**Department of Computer Applications ( M.C.A )**

**Course: MCA**

**Semester: II**

**Seminar Topic : Cybersecurity Threats and Protection**

**Submitted by:**

**USN:   2BA24MC007**

**Student Name:Anjali Hanamanth Dodamani**

**Date of Submission:26/06/2025**

**Guide/Faculty Name: Prof.S.M.Magi         Guide Signature:**

**Index Page**

**Table of Contents:**

**1.Introduction**

**2. Seminar Topic Details**

**3. Topic Summary**

**4. Relevance to MCA Curriculum**

**5. Learning Objectives**

**6. Expected Outcome**

**7. References**

**8. Signatures:**

1. **Introduction:**

In the digital age, cybersecurity has emerged as one of the most serious threats to individuals, organizations, and governments worldwide. Cybercriminals exploit vulnerabilities in computer systems and networks to steal sensitive information, disrupt operations, and commit fraud. These attacks range from phishing scams and ransomware to sophisticated breaches targeting critical infrastructure. As technology evolves, so do the methods of cyber attackers, making cybersecurity an essential priority. Protection against cybercrime involves a combination of technical measures, legal frameworks, and user awareness. Implementing strong security protocols, regularly updating systems, and educating users about cyber threats are key strategies in reducing risk and enhancing digital safetycyberattacks

**2.SEMINAR TOPIC DETAILS:**

Title: Cybersecurity Threats and Protection   
Area/Domain: identity theft, online fraud

Keywords: Cybercrime , Information security

# 3.Topic Summary:

essential for reducing risks and protecting sensitive data and systems from cyberattacks Cybersecurity threats and protection is a critical area of study in today’s digital world. It involves understanding various types of cyber threats such as malware, ransomware, phishing, identity theft, data breaches, and denial-of-service attacks, which can cause serious harm to individuals, businesses, and governments. These threats exploit vulnerabilities in systems, networks, or user behavior to steal information, disrupt services, or cause damage.

To combat these threats, cybersecurity protection includes a range of measures like firewalls, encryption, antivirus software, intrusion detection systems, and access control. It also involves implementing policies, security awareness training, and regular system updates. The primary goal is to safeguard digital systems by ensuring confidentiality, integrity, and availability of information.

As technology evolves, so do cyber threats. Therefore, staying informed and applying robust security practices are

# 4.Relevance to MCA Curriculum:

* **ComputerNetwork**  
   Understanding cybersecurity begins with knowing how data travels across networks. This subject helps students grasp networking protocols, IP addressing, and data transmission — all of which are critical in identifying and defending against network-based threats like packet sniffing, man-in-the-middle attacks, and DDoS.
* **OperatingSystem**  
  Operating systems manage system resources and user access. Cybersecurity is directly related to understanding OS vulnerabilities, access control mechanisms, and how malware or unauthorized access can exploit these systems.
* **InformationSecurity**  
  This subject is central to cyberseurity education. It covers core principles such as confidentiality, integrity, availability (CIA triad), risk management, security policies, and protection techniques like encryption and digital signatures

**5.Learning Objectives:**

* **Understand the nature and types of cybersecurity threats**: including malware, ransomware, phishing, social engineering, and advanced persistent threats (APTs).
* **Identify vulnerabilities in computer systems, networks, and applications** that can be exploited by cyber attackers.
* **Explain the core principles of information security** : confidentiality, integrity, and availability (CIA triad) — and how they relate to threat mitigation.
* **Analyze real-world cyberattacks and their impact** on individuals, businesses, and governments.
* **Apply encryption and cryptographic techniques** to protect sensitive data in transit and at rest

**6. Expected Outcome:**

* **Gain a thorough understanding of various cyber threats** and how they exploit vulnerabilities in digital systems.
* **Develop the ability to identify and assess cybersecurity risks** in different IT environment
* **Effectively implement and manage protection mechanisms** such as firewalls, encryption, and intrusion detection systems to safeguard information assets.
* **Demonstrate skills in responding to and mitigating cyber incidents**, including detecting attacks, containing damage, and recovering systems.
* **Apply cybersecurity best practices and frameworks** to design secure systems and networks.

**7. References:**

Author: Manish Gupta, John Walp, Raj Sharman **Source:** IGI Global

**Link:**[IGIGlobal-Threats,Countermeasures,andAdvances](https://www.igi-global.com/book/threats-countermeasures-advances-applied-information/60768" \t "_new)[en.wikipedia.org+4igi-global.com+4](https://www.igi-global.com/book/threats-countermeasures-advances-applied-information/60768?utm_source=chatgpt.com)

**Author:** Thomas A. Johnson **Publisher:** CRC Pres **Year:** 2015

**Authors:** Gulshan Shrivastava, Rudra Pratap Ojha, Shashank Awasthi, Kavita Sharma, Himani Bansal **Publisher:** Wiley-Scrivener **Year:** 2024 **Link:** [Wiley - Emerging Threats and Countermeasures](https://www.oreilly.com/library/view/emerging-threats-and/9781394230570/)[oreilly.com](https://www.oreilly.com/library/view/emerging-threats-and/9781394230570/?utm_source=chatgpt.com)[newyorker.com+9amazon.in+9oreilly.com+9](https://www.amazon.in/Cybersecurity-Essential-Knowledge-Dan-Shoemaker/dp/1435481690?utm_source=chatgpt.com)

**Coordinator Signature    HOD Signature**