ISSN: 2394-3122 (Online)
ISSN: 2394-6253 (Print)
Impact Factor: 6.03

Volume 12 Issue 12, December 2025

SK International Journal of Multidisciplinary Research Hub

Journal for all Subjects
e-ISJN: A4372-3088
p-ISJN: A4372-3089

Research Article / Survey Paper / Case Study
Published By: SK Publisher (www.skpublisher.com)

A Monthly Double-Blind Peer Reviewed Refereed Open Access Multidisciplinary & Multilingual International Journal - Included in the International Serial Directories

A Study on Cyber Security Threats and Prevention Techniques

Kalyani Raval[1]
Guide and Faculty,
Bachelor of Computer Application (B.C.A.),
M. J. College of Commerce,
Bhavnagar-364002, Gujarat, India

Nilam Tholiya[2]
Student,
Bachelor of Computer Application (B.C.A.),
M. J. College of Commerce,
Bhavnagar-364002, Gujarat, India

DOI: Available on author(s) request

Abstract: ***With the rapid growth of digital technologies and internet usage, cyber security has become a major concern for individuals, organizations, and governments. Cyber attacks such as malware, phishing, and data breaches are increasing day by day. This research paper studies various types of cyber security threats and discusses effective prevention techniques to protect data, systems, and networks from cyber attacks.***

Keywords: sensitive information, financial loss, cyber security.

I. INTRODUCTION

Cyber security refers to the protection of computer systems, networks, and data from unauthorized access, attacks, and damage. In today's digital world, most personal and business activities depend on online platforms. As a result, cyber threats have increased significantly.

Cyber criminals use different techniques to steal sensitive information, disrupt services, and cause financial loss. Therefore, understanding cyber security threats and their prevention techniques is very important.

II. CYBER SECURITY THREATS

Cyber security threats are harmful activities carried out by attackers to damage computer systems, networks, and data or to gain unauthorized access. With the increasing use of the internet and digital services, cyber threats have become more frequent and complex.

- **Malware:** Malware is malicious software designed to harm systems or steal information. It includes viruses, worms, trojans, spyware, and ransomware. Malware usually enters systems through infected files, email attachments, or unsafe websites.
- **Phishing:** Phishing attacks involve fake emails, messages, or websites that trick users into sharing sensitive information such as passwords, credit card details, or personal data.
- **Ransomware:** Ransomware is a type of malware that encrypts data and demands payment from the victim to restore access. It can cause serious financial and data loss.

- **Denial of Service (DoS and DDoS) Attacks:** In these attacks, attackers overload servers or networks with excessive traffic, making services unavailable to legitimate users.

III. Prevention Techniques

Cyber security threats can be reduced by implementing effective prevention techniques. These techniques help protect systems, networks, and data from unauthorized access and cyber attacks.

- **Strong Password and Authentication:** Users should create strong passwords using a combination of letters, numbers, and special characters. Multi-factor authentication (MFA) should be enabled to add an extra layer of security.
- **Regular Software Updates:** Operating systems, applications, and security software should be updated regularly to fix vulnerabilities and protect against new threats.
- **Antivirus and Anti-Malware Protection:** Installing reliable antivirus and anti-malware software helps detect and remove malicious programs before they harm systems.
- **Firewall and Network Security:** Firewalls help monitor and control network traffic, preventing unauthorized access to systems and networks.
- **Data Encryption:** Encryption converts sensitive data into an unreadable format, ensuring data safety even if it is stolen.

IV. Advantages of Cyber Security

Cyber security plays a vital role in protecting computer systems, networks, and data from cyber threats. It provides several benefits to individuals, organizations, and governments.

- **Protection of Sensitive Data:** Cyber security helps protect personal, financial, and confidential data from unauthorized access and data breaches.
- **Prevention of Cyber Attacks:** Strong security measures reduce the risk of attacks such as malware, phishing, and ransomware.
- **Financial Loss Prevention:** By preventing cyber crimes, cyber security helps avoid financial losses caused by fraud, data theft, and system downtime.
- **Data Integrity and Availability:** Cyber security ensures that data remains accurate, secure, and available to authorized users at all times.
- **Improved System Reliability:** Secure systems perform better and reduce the chances of crashes or failures due to cyber attacks.
- **User Trust and Confidence:** Strong cyber security builds trust among users and customers by ensuring safe digital services.

V. Challenges in Cyber Security

- Rapidly evolving cyber attacks
- Lack of skilled security professionals
- Poor user awareness
- High implementation cost

VI. Conclusion

Cyber security threats are increasing with the growth of digital technologies. Malware, phishing, ransomware, and insider threats pose serious risks to individuals and organizations. Implementing strong prevention techniques such as encryption, authentication, and user awareness can significantly reduce cyber security risks. A proactive approach is essential to ensure a safe digital environment.

References

1. Cyber Security and Infrastructure Security Agency (CISA)
2. NIST Cyber Security Framework
3. Research papers from Google Scholar

:::. Cite this article .:::

Kalyani Raval & Nilam Tholiya. (2025). A Study on Cyber Security Threats and Prevention Techniques. SK INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH HUB, 12(11), 23-25. https://skpublisher.com/docs/papers/volume12/issue12/SKV12I12-0004.pdf

