A.V.C COLLEGE OF ENGINEERING
DEPARTMENT OF COMPUTER APPLICATIONS

"CAS NEWS LETTER"

Volume: 30 **Month: March '26** **Issue: 1**

A Natural User interface (NUI) is a system for human-computer interaction that the user operates through intuitive actions related to natural, everyday human behavior. A NUI may be operated in a number of different ways, depending on the purpose and user requirements.

This is the emerging field in computer science. I encourage all the students to know about this kind of new technologies. This article is very much useful to about the methodologies involved in NUI

WISH YOU ALL SUCCESS...!!

DR.S.SELVAMUTHUKUMARAN

LEARNER-WRITER

SRIMATHI-II MCA

R.SIVASARASWATHI-II MCA

S.SRIPRADHA-II MCA

S.SIVAPRIYA-II MCA

V.SOWMIYA-II MCA

CYBER SECURITY

INTRODUCTION

Cyber security has become a fundamental part of our digital lives. As organisations and individuals increasingly rely on technology, cybercriminals continue to develop more sophisticated methods to steal data, disrupt services, and exploit vulnerabilities. Staying informed about emerging threats and adopting strong security practices are essential for protecting personal information, business assets, and critical infrastructure. This newsletter highlights the latest cybersecurity trends, common threats, and practical tips to help you stay secure online.

LATEST CYBERSECURITY TRENDS:

1. **AI-Powered Cyberattacks:** Attackers are using artificial intelligence to create convincing phishing emails, automate attacks, and bypass traditional security measures.
2. **Zero Trust Security:**Organisations are adopting Zero Trust models, where every user and device must be continuously verified before accessing resources.
3. **Cloud Security:** As cloud adoption grows, protecting cloud environments through encryption, identity management, and continuous monitoring has become a top priority.
4. **Ransomware Evolution:**Modern ransomware groups target businesses, hospitals, and government agencies with increasingly sophisticated attack techniques.

Common Cyber Threats:

Phishing:
Fraudulent emails, messages, or websites designed to trick users into revealing sensitive information such as passwords or banking details**.**

Malware:
Malicious software including viruses, worms, spyware, and trojans that can damage systems or steal confidential data**.**

Ransomware:
A type of malware that encrypts files and demands payment to restore access.

Social Engineering:
Psychological manipulation techniques used to convince people to reveal confidential information or perform actions that compromise security**.**

Insider Threats:
Security risks caused intentionally or unintentionally by employees, contractors, or trusted users.

Applications of Cyber security:

1. Banking & Finance:
Cyber security protects online banking, ATMs, digital payments, and financial transactions. It prevents unauthorized access, fraud, and theft of sensitive financial information.

2. Healthcare:
It protects patient medical records, hospital databases, and connected medical systems. Cyber security helps prevent data theft and unauthorized access to confidential information.

3. Education:
Educational institutions use cyber security to protect student records, examination systems, college portals, and research data. It also helps secure online learning platforms.

4. Business & Organizations:
Companies use cyber security to protect employee information, customer data, business applications, and internal networks. It helps reduce data breaches and cyber attacks.

5. E-Commerce:
Cyber security protects online shopping websites, customer accounts, payment details, and transactions. It helps customers safely purchase products and services online.

6. Mobile Applications:
Cyber security protects mobile apps and the personal information stored on smartphones. It helps prevent malware, unauthorized access, and account theft.

7. Cloud Computing:
Cloud security protects data, applications, and accounts stored on cloud platforms. It uses authentication, access control, and encryption to keep cloud resources secure.

8. Industrial Systems:
Industries use cyber security to protect machines, control systems, sensors, and industrial networks. This helps prevent disruptions and unauthorized control of critical systems.

9. Transportation:
Cyber security protects connected vehicles, railway systems, traffic management, and transportation databases. It helps prevent attacks that could affect transportation services.

10. Government & Defence:
Government organizations use cyber security to protect sensitive information communication systems, and critical infrastructure. It helps defend against cyber espionage and other cyber threats.

11. IoT Devices:
Cyber security protects smart cameras, smart homes, wearable devices, sensors, and other connected devices. It prevents attackers from gaining unauthorized access to these devices.

12. Social Media:
Cyber security helps protect social media accounts, personal information, messages, and digital identities. Strong passwords, privacy settings, and 2FA can improve account security.



Advantages of Cyber Security:

- **Data Protection** :Cybersecurity protects important personal and organizational data from theft, loss, and unauthorized access.
- **Prevents Cyber Attacks**:It helps prevent threats such as hacking, malware, phishing, ransomware, and other online attacks.
- **Privacy Protection** :It keeps sensitive information like passwords, personal details, and financial data safe from unauthorized users.
- **Financial Security** :Cybersecurity reduces the risk of online fraud, financial theft, and other cyber-related monetary losses.
- **Builds Trust** :Strong cybersecurity increases the confidence of customers and users by ensuring that their information is secure.

Data Privacy and Protection:

Data privacy and protection means keeping personal and sensitive information safe from unauthorized access, misuse, theft, or loss. It ensures that data is collected, stored, and shared responsibly.

Important Data Protection Practices:

- Use strong passwords and **Two-Factor Authentication (2FA)**.
- Encrypt sensitive information.
- Avoid sharing personal information with unknown websites or people.
- Keep software and security systems updated.
- Take regular backups of important data.
- Use secure networks when accessing sensitive information.

Password Security:

Password security is the practice of creating and protecting strong passwords to prevent unauthorized access to accounts and personal information. A strong password should be difficult to guess and should not contain easily available information such as your name or birthday.

Important Password Security Tips:

- Use long and unique passwords for different accounts.
- Combine **uppercase, lowercase, numbers, and special characters**.

Never share your passwords with others.

- Avoid using the same password on multiple websites.
- Enable **Two-Factor Authentication (2FA)** whenever possible.
- Use a trusted **password manager** to store passwords securely.
- Change passwords if you believe an account has been compromised.

Network Security

Network security is the practice of protecting computer networks and connected devices from unauthorized access, cyber attacks, malware, and data theft. It helps ensure that information travels safely across a network.

Important Network Security Methods:

- Use **firewalls** to block unauthorized network traffic.
- Use **encryption** to protect data during transmission.
- Install and regularly update antivirus and security software.
- Use strong Wi-Fi passwords and secure network settings.
- Monitor network activity to detect suspicious behavior.
- Keep operating systems and network devices updated.

Online Banking & Payment Safety

Digital payments are convenient, but users should remain careful.

Important rules:

- Never share OTPs, PINs, or passwords.
- Verify payment requests before approving them.
- Don't install apps at the request of unknown callers.
- Check the recipient before sending money.
- Avoid suspicious links claiming to provide refunds or rewards.
- Contact the bank through its official channels if something looks suspicious.

Firewall and Antivirus

Firewall and **antivirus** are important cybersecurity tools that protect computers and networks from different types of cyber threats.

Firewall:

- Monitors incoming and outgoing network traffic.
- Blocks unauthorized or suspicious connections.
- Helps prevent attackers from accessing a device or network.
- Can be hardware-based or software-based.

Antivirus:

- Detects and removes malware such as viruses, trojans, and spyware.
- Scans files, applications, and devices for threats.
- Provides real-time protection against suspicious activities.
- Should be regularly updated to detect new threats.

Encryption and Cryptography

Encryption and cryptography are important cybersecurity techniques used to protect information from unauthorized access. They help keep sensitive data secure while it is stored or transmitted.

Encryption:

- Converts readable data (**plaintext**) into an unreadable format (**ciphertext**).
- A key is used to encrypt and decrypt the data.
- Protects sensitive information such as passwords and financial data.
- Commonly used in secure websites, messaging apps, and online transactions.

Cryptography:

- Uses mathematical techniques to secure information and communication.
- Includes **encryption, decryption, hashing, and digital signatures**.
- Helps provide confidentiality, data integrity, authentication, and non-repudiation.

Cyber Crime and Cyber Law

Cyber crime refers to illegal activities carried out using computers, smartphones, networks, or the internet. **Cyber law** consists of legal rules and regulations created to prevent cyber crimes and protect people, organizations, and digital information.

Examples of Cyber Crimes:

- Hacking and unauthorized access
- Online identity theft
- Phishing and online scams
- Cyberbullying and online harassment
- Data theft and privacy violations
- Malware and ransomware attacks

Cyber Law:

- Provides legal protection for digital data and online activities.
- Defines punishments for various cyber crimes.
- Helps investigate and prosecute cyber criminals.
- Protects users' privacy and digital rights.
- Regulates activities such as electronic transactions and digital signatures.

Major Areas of Cyber Law:

- Data protection and privacy
- Online fraud and financial crimes
- Unauthorized computer access
- Electronic records and digital transactions
- Intellectual property protection
- Cyber harassment and abuse
- Digital signatures and authentication

Cyber Law in India

In India, the **Information Technology Act, 2000 (IT Act)** is a major law dealing with electronic records, electronic transactions, and several cyber offences. Other laws may also apply depending on the nature of the offences.

Conclusion:

Cyber security has become an essential part of modern technology because almost every activity todaydepends on computers, smartphones, networks,cloud platforms, and the Internet. Organizations store large amounts of valuable information such as personal details, financial records,business data, passwords, and confidential documents in digital systems.
Therefore, protecting these systems from unauthorized access, data theft, malware, phishing, ransomware,and other cyber attacks is extremely important.
Cyber security is not limited to installing antivirus software or using strong passwords. It is a **continuous process**that involves protecting hardware, software, networks, applications, data, and users. Effective cyber securityrequires a combination of technologies, security policies, regular monitoring, employee awareness, risk assessment,
and proper incident-response procedures.

Future of cyber security:

The future of cyber security is very broad because new technologies create both opportunities and new security challenges. Some important areas of future development are:

Artificial Intelligence and Machine Learning:

- Artificial Intelligence (AI) and Machine Learning (ML) will play an important role in future cyber security.
- AI systems can analyze huge amounts of network and system data much faster than humans.
- They can identify unusual behavior and potentially detect attacks at an early stage.

For example:

Normal activity → AI monitoring → Unusual activity detected → Security alert → Investigation

Rush your ideas to
P. JAYAPAL MCA., M.Phil.,
Assistant Professor/CA Editor-
CAS Mail-
Id:editor.cas@gmail.com,
pjavcce@gmail.com