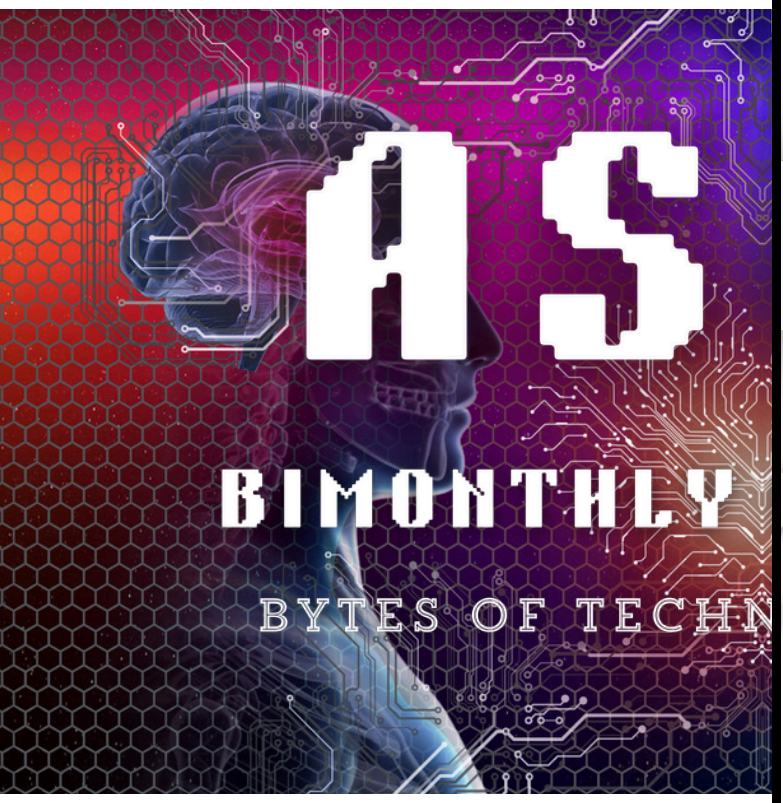
MARCH 15, 2025



ABOUT ASCII

ASCII Newsletter is a student-driven, bimonthly publication celebrating innovation, technology, and creativity. While created by students, it's designed for anyone with a keen interest in technology- offering thoughtfully selected articles, hands-on tutorials, and the latest tech updates to engage and empower all curious minds.

Editorial Board

Chief Editor

Mr. Tanishq Sharma
F.Y.B.Sc. CS

Technical Content Lead

Mr. Vineet Khamrai
Assistant Professor

Design & Layout Lead

Ms. Jeenal Jain
Assistant Professor

Mr. Aakash Verma
Assistant Professor

Design & Editor

Ms. Maanya Poojary
F.Y.B.Sc. CS

Contributors

Mr. Aditya Sukhal
F.Y.B.Sc. CS

Mr. Shankar Singh
F.Y.B.Sc. CS

Ms. Gauri Pednekar
F.Y.B.Sc. CS

Ms. Archana Jha
F.Y.B.Sc. IT

Ms. Ananya Bhogal
F.Y.B.Sc. IT

Editors

Dr. Bhakti Chaudhari
Coordinator of B.Sc. CS

Ms. Vaishali Mishra
Coordinator of B.Sc. IT

MARCH 15, 2025

VOLUME 1
ISSUE: 04

ABOUT ASCII

ASCII Newsletter is a student-driven, bimonthly publication celebrating innovation, technology, and creativity. While created by students, it's designed for anyone with a keen interest in technology- offering thoughtfully selected articles, hands-on tutorials, and the latest tech updates to engage and empower all curious minds.

WHAT'S INSIDE ?

+91 77150 91244

nmfdegree.edu.in

Nirmala Memorial Foundation
COLLEGE OF COMMERCE & SCIENCE

VOLUME 1
ISSUE : 04

MARCH 15, 2025

Early Concept of Cyber-Security

Tentative Ideas about IT Security: During the very first computing years, there was little emphasis on "cybersecurity," because computers were solitary devices used mostly for scientific research or military activities. Typical security issues related to the computers and the data were centered on the physical connection to the computers.

Primitive Steps Towards IT Security: Once computers were employed for more functional activities (like business and finances), the idea of privacy and access control began to take shape. The initial systems had primitive security measures in place, including the use of physical locks and weak authentication mechanisms where usernames and passwords were required to gain access.

EXPANSION OF CYBER SECURITY:

As internet usage grew exponentially, so did cyberattacks, leading to more advanced cybersecurity measures.
The early 2000s saw the rise of sophisticated threats like worms, phishing, and spyware. Governments and private companies started investing heavily in developing cybersecurity strategies and technologies to protect against these emerging threats. As businesses and individuals became more reliant on the internet for communication, e-commerce, cloud storage, and other activities, the need to protect online data became crucial. This led to the development of firewalls, encryption methods, intrusion detection systems, and other tools designed to secure online communications and transactions.

Do You Know?

First Computer Virus (1971): One of the earliest computer viruses, also known as computer programs that propagate from one device to another, was developed by Bob Thomas while working for BBN Technologies. It was dubbed the Creeper virus and was meant to be a harmless Kotlin experiment aimed at determining if a computer program could traverse over a network. This served as a starting point to what is now recognized as 'malware.'

-Ananya Bhogal
(F.Y.B.S.c.I.T)

As internet usage grew, so did cyberattacks, prompting the development of advanced cybersecurity measures. In the early 2000s, sophisticated threats like worms, phishing, and spyware emerged, leading governments and private companies to invest heavily in cybersecurity. As reliance on the internet for communication, e-commerce, and cloud storage increased, safeguarding online data became critical. This spurred the creation of firewalls, encryption methods, and intrusion detection systems to protect online communications and transactions.

Nirmala Memorial Foundation
COLLEGE OF COMMERCE & SCIENCE

VOLUME 1
ISSUE : 04

MARCH 15, 2025

Phishing: A Growing Cyber Threat

How to Protect Yourself !

Enable-Multi-Factor Authentication (MFA) to add an extra security layer.

Keep software and antivirus updated to protect against malware.

Use strong and unique passwords to secure accounts.

Educate employees and individuals or recognizing phishing threats.

Report phishing attempts to authorities or IT teams to prevent further attacks.

Phishing is a type of cyber scam where criminals impersonate trusted organizations, such as banks, government agencies, or well-known companies, to steal sensitive information like passwords, credit card numbers, and personal identification details. These attacks are designed to deceive victims by creating a sense of urgency or fear, convincing them to take immediate action — such as clicking a link, downloading an attachment, or providing confidential information. The stolen data is then misused for fraud, identity theft, and other criminal activities.
Phishing tactics have become increasingly sophisticated, making it harder to distinguish legitimate communications from fraudulent ones. Cybercriminals often tailor their messages using personal details obtained from public sources or previous data breaches to make their attacks more convincing

Phishing attacks come in various forms, exploiting different communication channels and human vulnerabilities.
Phishing emails are the most common, where criminals send fake emails from trusted sources like banks or online services, often using alarming language and malicious links to steal credentials. **Fake websites** mimic legitimate ones, tricking users into entering sensitive information.
Smishing involves fraudulent text messages with suspicious links or urgent requests, while vishing uses scam phone calls where criminals pose as trusted representatives to steal personal details. **Social media phishing** includes fake giveaways, impersonations, and malicious links shared through direct messages or comments. To protect yourself, verify sources, avoid clicking unknown links, enable two-factor authentication, stay cautious, and report suspicious activity.

DID YOU KNOW?

How to Identify Phishing Attempts?

- Suspicious email addresses
- Urgent or threatening messages
- Fake links
- Grammatical errors
- Unexpected requests for sensitive data source before responding.

– Aditya Sukhal
F.Y.B.S.c.CS

Nirmala Memorial Foundation
COLLEGE OF COMMERCE & SCIENCE

VOLUME 1
ISSUE : 04
MARCH 15, 2025

Practices for Protecting Personal Data

Quick Tips:

Avoid reusing passwords across accounts.

Set up login alerts.

Educate yourself and your family about online scams !

Recent Breach Highlights:
A major social media platform exposed 500 million records.

A healthcare provider faced a ransomware attack, putting patient data at risk.

Following these simple yet effective practices can significantly reduce your vulnerabilitycyberattacks. Start today and keep your personal data safe!

–Tanishq Sharma
F.Y.B.S.c.CS

In today's digital world, personal data is a prime target for cybercriminals. With over 5 billion records exposed in 2024 alone, securing your personal information — like passwords, financial details, and social media activity — is more crucial than ever. Here's how you can protect yourself:

Top 6 Data Protection Practices:
Use Strong Passwords: Create unique passwords with a mix of letters, numbers, and symbols. Use a password manager to keep them secure. Enable **Multi-Factor Authentication (MFA):** Adds an extra layer of security beyond just a password. **Keep Software Updated:** Regular updates fix security vulnerabilities. Avoid Public Wi-Fi: Use a VPN to protect your data on unsecured networks. **Monitor Your Accounts:** Check for unusual activity and set up alerts for suspicious logins. **Watch for Phishing:** Don't click suspicious links or respond to unknown emails. Limit Social Media Sharing: Be mindful of the personal information you share online. Secure Your Devices: Use passcodes, fingerprint scans, and remote wipe options.
Back Up Your Data: Regular backups protect against data loss. Use Encrypted Messaging: Apps like Signal and WhatsApp keep your conversations private.

Nirmala Memorial Foundation
COLLEGE OF COMMERCE & SCIENCE

VOLUME 1
ISSUE : 04
MARCH 15, 2025

Emerging Cybersecurity Trends in 2025

Cybersecurity Trends Quiz

Which technology is used to enhance real-time threat detection and response?

A) Blockchain
B) AI and Machine Learning
C) VPN
D) Firewall

-Archana Jha
F.Y.B.S.c.I.T

Key Cybersecurity Trends Shaping 2025

As cyber threats grow more advanced, organizations need to strengthen their defenses and adapt to new risks. Here are the key cybersecurity trends expected to impact industries in 2025:

- **AI in Cybersecurity**

Artificial Intelligence (AI) is playing a dual role in cybersecurity. While AI helps automate threat detection and quick response, cybercriminals are also using AI to create smarter attacks like deepfake scams and phishing. To stay ahead, businesses must adopt AI-based defense strategies.

- **Zero Trust Architecture (ZTA)**

The traditional security model of trusting internal systems is no longer effective. The Zero Trust model assumes that threats can come from both inside and outside the network. Organizations are implementing multi-factor authentication (MFA), limited access permissions, and continuous monitoring to secure their systems.

- **Ransomware as a Service (RaaS)**

Ransomware attacks are increasing, with hackers now selling ransomware tools to non-experts. This makes attacks easier to launch and more damaging. Businesses need stronger endpoint protection, regular backups, and employee training to reduce risks.

- **Quantum Computing and Encryption Risks**

Quantum computers could soon break current encryption methods, making sensitive data vulnerable. Companies are working on quantum-resistant encryption to secure future data.

- **IoT Security**

The growing use of smart devices (like home assistants and industrial sensors) creates more security gaps. Stronger encryption, better user authentication, and network segmentation are needed to protect IoT systems.

- **Supply Chain Attacks**

Cybercriminals are targeting suppliers and service providers to attack multiple businesses at once. Strengthening supplier security policies, conducting regular audits, and monitoring for vulnerabilities can help prevent such breaches.

- **New Regulations and Compliance**

Governments are introducing stricter cybersecurity laws to protect user data and privacy. Businesses need to follow regulations like GDPR and CCPA to avoid penalties and protect customer information.

The future of cybersecurity will require a proactive approach, combining AI, advanced encryption, and stronger security policies to stay ahead of evolving threats.

Nirmala Memorial Foundation
COLLEGE OF COMMERCE & SCIENCE

VOLUME 1
ISSUE : 04
MARCH 15, 2025

The Future of Cybersecurity: Key Innovations, Challenges, and Industry Impact

The future of cybersecurity will be shaped by advancements in Artificial Intelligence (AI), Machine Learning (ML), and quantum computing. AI and ML are enhancing threat detection and response by analyzing user behavior and identifying suspicious activity in real time. Post-quantum cryptography is becoming essential as quantum computers pose a threat to existing encryption methods, prompting the development of quantum-resistant security solutions. Cybersecurity mesh, which integrates multiple security systems into a unified framework, is improving adaptive protection across networks and devices. The adoption of Zero Trust Architecture, which requires continuous authentication and strict access controls, is also becoming standard to minimize insider threats and unauthorized access. Cloud security is gaining importance as businesses migrate to cloud environments, requiring enhanced encryption, monitoring, and identity management.

However, the cybersecurity landscape faces growing challenges. Ransomware attacks targeting critical infrastructure and financial institutions are becoming more sophisticated. Supply chain attacks, where third-party vendors are compromised, pose a significant threat to business networks. Weak security in Internet of Things (IoT) devices creates new vulnerabilities, while deepfake technology and social engineering attacks are exploiting human psychology to manipulate individuals and systems.

Cybersecurity Across Industries (2025 Projections)
By 2025, cybersecurity will play a vital role in protecting data and infrastructure across various sectors:

- Healthcare
- Finance
- Retail & E-commerce
- Manufacturing
- Government & Defense
- Energy & Utilites
- Education & Research

-Gauri Pednekar
(FY.BSc.CS)

Innovative solutions are emerging to combat these threats. AI-driven behavioral analytics can detect anomalies and prevent attacks in real time. Satellite cybersecurity is becoming critical as satellite-based communication and navigation systems face increasing risks. Biometric security, including fingerprint, facial, and voice recognition, is strengthening identity verification and access control.

The impact of cybersecurity will be felt across industries. In healthcare, securing patient data and connected medical devices will be a top priority. Financial services will focus on fraud prevention and secure transactions. The manufacturing sector will work to protect industrial systems from sabotage and espionage. Government and defense will prioritize securing national infrastructure and military networks against state-sponsored attacks.

The global cybersecurity market is projected to exceed $300 billion by 2026 as governments and businesses invest in adaptive security frameworks and quantum-resistant encryption. Collaboration between industry leaders and governments will be essential to staying ahead of evolving threats and ensuring a secure digital future.

Accolades

We are thrilled to announce the incredible success of our TYIT students who have secured placements through the recent college job fair! Your hard work, dedication, and determination have truly paid off, and we couldn't be prouder of your achievements.

Our Star Achievers:

- **Shubham Misal – Placed at Property Plaaza**
- **Vaijayanta Chikke – Placed at Property Plaaza**
- **Shrutaj Poojary – Placed at Sutherland Global Services**
- **Aaryan Sawardekar – Placed at Sutherland Global Services**

Securing a job placement is a significant milestone, and it reflects not only your academic excellence but also your commitment to building a strong foundation for your future career. The skills and knowledge you've gained throughout your journey in BSc-IT have prepared you well for the challenges and opportunities that lie ahead.

- **The Road to Success**

The placement process is never easy — it requires months of preparation, persistence, and a strong mindset. From honing technical skills to mastering communication and interview techniques, you have shown remarkable dedication. The confidence and professionalism you displayed during the job fair have truly set you apart.

- **A Bright Future Awaits**

This is just the beginning of your professional journey. The experiences and lessons you've learned during this process will serve as a strong foundation for future growth. Remember that every challenge you face is an opportunity to learn and grow. Keep pushing boundaries, setting new goals, and striving for excellence.

- **A Message of Gratitude and Encouragement**

We would also like to extend our heartfelt gratitude to the recruiters and companies who recognized the potential and talent of our students. To all our students, let this achievement serve as motivation to keep working hard and aiming high.

Congratulations once again on this well-deserved success! We are confident that you will continue to make us proud and inspire future batches with your accomplishments. Keep aiming high and believing in your abilities — the future is bright!

Best wishes,
Vaishali Mishra
BSc-IT Coordinator

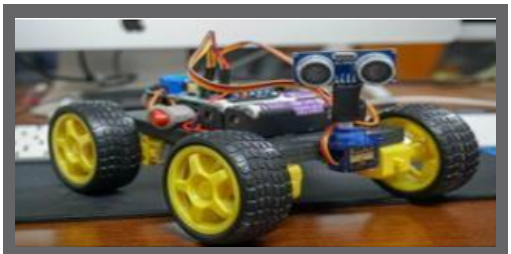
Nirmala Memorial Foundation
COLLEGE OF COMMERCE & SCIENCE

VOLUME 1
ISSUE : 04

MARCH 15, 2025

Innovative Creations by Students: Empowering Learning and Community Care

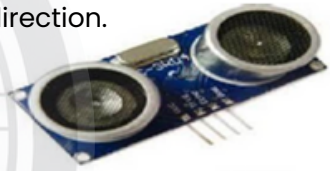
1. SonicScout: Autonomous Obstacle-Avoiding Car Using Arduino



Sonic Scout
Swapnil jain
T.Y.B.Sc. CS

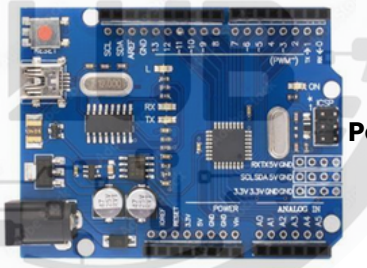
SonicScout is an autonomous robotic vehicle designed using an Arduino microcontroller, ultrasonic sensors, and servo motors to detect and avoid obstacles in real-time. The ultrasonic sensor sends data to the Arduino, which processes it and adjusts the car's movement using servo motors for smooth navigation. A buzzer provides auditory feedback when obstacles are detected, improving user awareness. The system operates wirelessly using a rechargeable battery for enhanced mobility and convenience.

- Arduino Uno – Acts as the microcontroller, processing real-time data from the sensors.
- Ultrasonic Sensor – Measures distance and detects obstacles using sound waves.
- Servo Motors – Adjust the position of the ultrasonic sensor for improved scanning.
- Motor Driver (L298N) – Controls the DC motors for movement and direction.
- DC Motors – Enable forward, backward, and turning movements.
- Buzzer – Provides auditory feedback when obstacles are detected.
- Power Supply – Powered by 18650 batteries for wireless operation.



Ultrasonic Sensor

DC Motor



Power Supply

The system design and coding of SonicScout are based on the Arduino IDE, where the code is written using C++ libraries such as Servo.h and NewPing.h. The robotic car follows a structured decision-making algorithm to navigate its environment effectively. When an obstacle is detected, SonicScout immediately stops and scans the left and right sides using servo motors. Based on the input, it decides to turn toward the open side or reverse if no clear path is available, ensuring smooth and efficient navigation.

The project is highly feasible across technical, economic, operational, and schedule aspects. It uses accessible components and open-source software, with an estimated cost of $30 to $100 and minimal user input, making it easy to develop and operate. A working prototype can be built within 1 to 2 weeks. Future enhancements include AI integration for smarter decision-making, pathfinding algorithms like A* and Dijkstra's for better navigation, and object recognition through computer vision for improved accuracy. Ensuring compliance with safety standards will enhance system reliability for real-world applications.

2. “Everything about Students”

“Everything About Students”
Atul Mishra
T.Y.B.Sc. CS

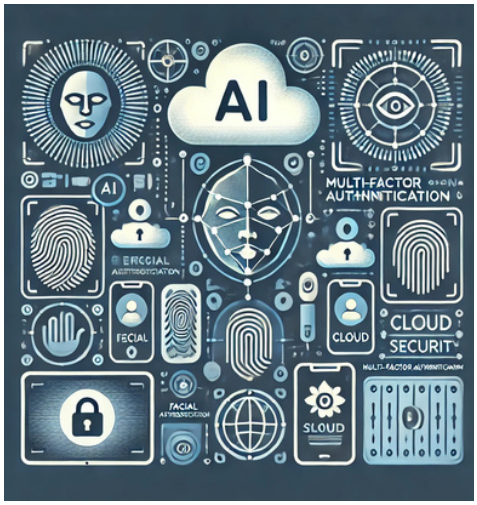
The project introduces an automated attendance system using facial recognition technology to improve accuracy and efficiency in attendance tracking. A smartphone camera captures real-time images or videos, which are processed using advanced algorithms to identify individuals by matching them with a pre-registered database. This eliminates the need for manual roll calls, saving time and reducing errors. The system works reliably under various lighting conditions and generates detailed reports instantly. It can also integrate with existing Learning Management Systems (LMS) or corporate databases, making it scalable and adaptable for educational and professional settings.

The project aims to automate attendance tracking using facial recognition technology to improve accuracy and efficiency while reducing human error. It eliminates fraud like buddy punching by ensuring only the rightful individual is marked present. The system provides real-time processing and generates detailed reports for better decision-making. It ensures data security through encryption and access control, while its scalable design allows it to adapt to various environments, such as classrooms and offices, handling increasing user numbers efficiently.

- **Which technology is used for real-time facial recognition in the project?**

The project utilizes a robust technology stack to ensure high performance and scalability. The frontend is developed using React.js, HTML, CSS, and JavaScript to create a responsive and dynamic user interface with real-time updates. The backend is powered by Node.js with Express.js, enabling fast data processing and efficient API management. MongoDB serves as the database, allowing the system to handle large data volumes with ease. For facial recognition, the project integrates OpenCV and machine learning models, ensuring real-time, accurate attendance tracking with high reliability and precision.

- **What is one future improvement planned for the attendance system?**



The project’s future scope focuses on improving both functionality and security. AI-based emotion detection will analyze user engagement and behavior during attendance tracking, providing deeper insights into user interactions and enhancing system intelligence. To strengthen security, multi-factor authentication will be implemented, combining facial recognition with OTP or biometric data to ensure that only authorized users can access the system. Migrating to cloud-based storage will enhance scalability and allow seamless data access and synchronization across devices, enabling the system to handle large datasets more efficiently. Additionally, enhanced deep learning models will improve recognition accuracy even in low-light or obstructed conditions, making the system more reliable and adaptable for real-world use.

Languages in Cyber-Security !

- **Python** is one of the most widely used languages in cybersecurity due to its simplicity, extensive libraries, and powerful scripting capabilities.
- **C** allows cybersecurity professionals to understand and manipulate system-level processes. Many vulnerabilities, such as buffer overflows, originate from C-based applications.
- **C++** is used for high-performance security applications and helps in understanding how malware and advanced persistent threats (APTs) function.
- **PHP** powers many web applications, making it a prime target for attackers. Understanding PHP helps in securing web applications.
- **JavaScript** is widely used for building websites and web applications. Hackers often target JavaScript to find security weaknesses in websites.
- **Java** is used to create large business applications and secure Android devices. Learning Java helps in protecting enterprise systems and mobile apps.
- **Bash** is a scripting language used in Linux and Unix systems. It helps automate security tasks like monitoring and managing files. Cybersecurity experts use Bash to improve system security and efficiency.
- **SQL** is used to manage databases that store important information. Hackers often try to break into databases using SQL injection attacks. Understanding SQL helps in securing databases from such threats.

Nirmala Memorial Foundation
COLLEGE OF COMMERCE & SCIENCE

VOLUME 1
ISSUE : 04
MARCH 15, 2025

Job Opportunities in Cyber Security!

Cybersecurity focuses on protecting systems, networks, and data from online threats. As companies rely more on technology, skilled professionals are in high demand. Jobs include ethical hacker, security analyst, and risk manager across industries like government, banking, healthcare, and tech. Skills in penetration testing, cloud security, and threat analysis are valuable. The field offers good pay, remote work options, and ongoing learning opportunities. Certifications can help advance your career.

• Why Consider a Career in Cyber Security

Cybersecurity is in high demand due to rising cyber threats, making skilled professionals essential for protecting organizations. It offers competitive pay, especially in specialized fields like hacking and cloud security. Career options include roles like security engineer and consultant across industries such as finance, healthcare, and tech. The field evolves constantly, requiring ongoing learning to stay ahead of threats. Jobs are stable since secure systems are critical for businesses. Many positions offer remote work and flexible hours. Entry is accessible through certifications and experience, even without a formal degree. This makes cybersecurity a rewarding and dynamic career choice.

• Explore the Future of Work in Cyber Security

Cybersecurity will increasingly rely on automation and AI to counter smarter cybercriminals. Cloud security, Zero Trust models, and skilled experts will be crucial. Privacy laws will push businesses to protect data better, while new tech like IoT, 5G, and blockchain will create new security challenges. Cybersecurity will become central to business trust and reputation, driving more collaboration between governments and companies. The field will continue evolving, offering new opportunities and challenges.

• In-Demand Skills for Cyber Security

Cybersecurity pros need key skills to handle modern threats. Threat intelligence helps predict dangers, while network and cloud security protect systems and data. Incident response and forensics fix issues after attacks. Penetration testing exposes weak spots, and risk management ensures compliance. Cryptography secures sensitive data, while automation and scripting improve threat detection. Zero Trust models require strict access checks, and security operations manage daily security tasks. These skills are vital to tackling today's complex cyber challenges.

Facts

- Cyberattacks are becoming more common. Things like ransomware and phishing are happening a lot more often because cybercriminals keep changing how they attack.
- Cybersecurity matters to everyone. Whether you're a hospital or a bank, hackers are after your data. Even if you run a small shop, you're still a target. So, no matter how big or small you are, you need to take security seriously.
- Data breaches can really hit your wallet hard. We're talking millions on average for fixing things, legal stuff, and the hit your reputation takes.
- Governments worldwide are making data protection and cybersecurity rules tougher. Think GDPR and CCPA – they're all about keeping your personal info safe and making sure companies are responsible with it.

Nirmala Memorial Foundation
COLLEGE OF COMMERCE & SCIENCE

VOLUME 1
ISSUE : 04
MARCH 15, 2025

PUZZLE TIME

CAN YOU GUESS THE RIDDLE?

1. I guard your digital gates, making sure only trusted users pass while others wait. What am I?

2. I'm a sneaky email, pretending to be real, but one click on me, and your data I steal. What am I?

3. I'm the fortress around your secrets, scrambling them so no one can read it. What am I?

4. I'm the password's smarter sibling, an extra step to keep bad guys from slipping.

5. I'm like a magic tunnel, hiding your data's journey from start to end. What am I?

6. I hide behind your screen, logging every keystroke with unseen schemes. What am I?

7. I'm like a lock, but you forget me more often than your socks! What am I?

8. A cyber villain I am, spreading havoc when I land, multiplying without your command. What am I?

Hints

Hardware, urgent action or threat, special character, two ways, protect you, personal security, viral

Wordsearch - Mind Maze !

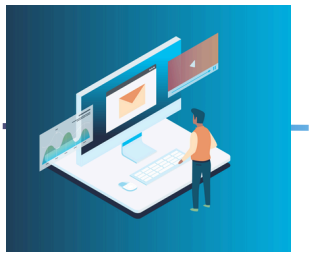
K	F	S	U	E	M	A	I	L	T
H	P	N	D	P	N	T	N	G	R
K	H	I	A	Z	E	N	T	D	U
O	I	V	T	V	M	T	E	R	Y
C	S	H	A	C	K	E	R	E	B
O	H	N	L	S	N	I	N	N	M
O	B	O	E	P	I	B	E	C	A
K	T	V	S	T	R	N	T	Y	L
I	O	I	A	T	W	I	E	Y	W
E	W	R	P	A	G	O	H	P	A
S	U	P	D	A	T	E	R	T	R
P	A	S	S	W	O	R	D	K	E

Words to Search

- Update
- Cookies
- Encrypt
- Email
- Internet
- Password
- Phish
- Malware
- Data
- Hacker
- Virus
- Network

CARRER IN CYBER SECURITY

Security Engineer



CyberSecurtiy Analyist

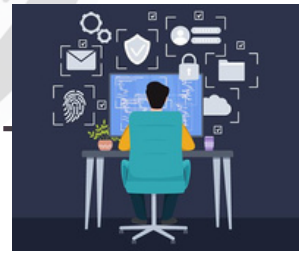
Penetration Tester

Ethical hacker

Information Security Analyist

Cloud Security

Computer forensics Engineer



Cyber Security Speciallist

Data Privacy Officer

MARCH 15, 2025 ISSUE : 04 VOLUME 1

ASCII

BIMONTHLY NEWSLETTER

BYTES OF TECHNOLOGY & TRENDS

TECH ENTHUSIASTS CAN SHARE THEIR ARTICLES AND CONTENT FOR THE NEWSLETTER AT :techclub@nirmala.edu.in

+91 77150 91244

nmfdegree.edu.in