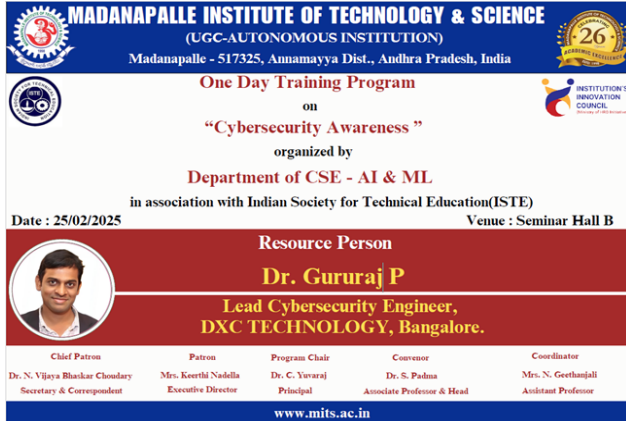


A Report on One Day Training Program on "Cybersecurity Awareness"
Organised by
Department of CSE- Artificial Intelligence & Machine Learning
on 25.02.2025



MADANAPALLE INSTITUTE OF TECHNOLOGY & SCIENCE
(UGC-AUTONOMOUS INSTITUTION)
Madanapalle - 517325, Annamayya Dist., Andhra Pradesh, India

One Day Training Program
on
"Cybersecurity Awareness"
organized by
Department of CSE - AI & ML
in association with Indian Society for Technical Education (ISTE)
Date : 25/02/2025 Venue : Seminar Hall B

Resource Person
Dr. Gururaj P
Lead Cybersecurity Engineer,
DXC TECHNOLOGY, Bangalore.

Chief Patron Dr. N. Vijaya Bhaskar Choudary Secretary & Correspondent	Patron Mrs. Keerthi Nadella Executive Director	Program Chair Dr. C. Yuvaraj Principal	Corector Dr. S. Padma Associate Professor & Head	Coordinator Mrs. N. Geethanjali Assistant Professor
------------------------------------------------------------------------------------	-------------------------------------------------------------	-----------------------------------------------------	---------------------------------------------------------------	------------------------------------------------------------------

www.mits.ac.in



Report Submitted by: Mrs. N. Geethanjali, Assistant Professor, Department of CSE – AI & ML.
Resource person Details Dr. Gururaj P-Lead Cybersecurity Engineer, DXC Technology, Bangalore.
Participants: II Year CSE – AI & ML & CSE –Networks – 100 ISTE Student Member
Venue: Seminar Hall B
Mode of Conduct: Offline
Report Received on 01.03.2025.

Department of Computer Science & Engineering – AI & ML has organized a One Day Training Program on Cybersecurity Awareness on 25/02/2025(Tuesday).

Welcome Address:

The event commenced at 10:00 AM with a warm and engaging welcome address to all by Mrs. N. Geethanjali, Asst. Professor, Department of CSE – AI & ML, Madanapalle Institute of Technology & Science (MITS), Madanapalle. The Indian Society for Technical Education (ISTE) is a national organization that promotes the growth of technical education in India. It supports educators and students through conferences, workshops, and industry collaborations. ISTE aims to enhance the quality of engineering and technology education across the country.



Keynote Address:

Dr. S. Padma, Associate Professor & Head, Department of CSE – AI & ML, Madanapalle Institute of Technology & Science (MITS), Madanapalle. The Head of Department (HOD) in ISTE event typically emphasizes the importance of innovation and research in technical education. Highlighting the growing cyber threats and the need for awareness. The session focused on real-world cybersecurity cases and the impact of cyber threats on individuals and organizations. The HOD also encourages students to actively participate in ISTE activities to enhance their skills and broaden their horizons.

Dr. P. Ramanathan, Professor, ECE, Vice Principal – Academics, MITS, Madanapalle explained about the Today's training program is a significant step toward equipping ourselves with the knowledge and skills needed to mitigate cyber risks. It is essential for all of us whether we are professionals, students, or business owners to understand the basics of cybersecurity and how to safeguard our digital presence.

I commend the organizers for taking this initiative and providing a platform to discuss this critical subject. I also encourage all participants to actively engage in today's sessions, ask questions, and implement the knowledge gained to enhance cybersecurity in their respective domain.

Resource Person Lecture:

Dr. Gururaj P-Lead Cybersecurity Engineer, DXC Technology, Bangalore. He explained about the importance of ISTE and how can we utilize that membership. A resource person speaking about the internet has revolutionized the way we work, communicate, and conduct business. However, with great opportunities come great risks. Cyber threats such as phishing, ransomware, data breaches, identity theft, and cyberbullying have become rampant. Organizations, governments, and individuals are all vulnerable to cyberattacks, making cybersecurity awareness more crucial than ever before.

Here are a few key aspects I would like to emphasize:

- **Strong Passwords and Authentication** – Simple passwords make it easier for cybercriminals to gain access to our accounts. Using strong, unique passwords and enabling multi-factor authentication (MFA) can add an extra layer of security.
- **Recognizing Phishing Attempts** – Cybercriminals often use deceptive emails, messages, or websites to steal sensitive information. Being vigilant and verifying sources before clicking on links or downloading attachments can prevent cyber fraud.
- **Safe Internet Practices** – Avoid accessing sensitive accounts over public Wi-Fi, ensure software updates are installed regularly, and use secure and legitimate applications.
- **Data Protection and Privacy** – Personal and professional data should be stored securely. Organizations must implement encryption and backup strategies to prevent data loss and leakage.
- **Awareness and Education** – Cybersecurity is a continuous learning process. Regular training and awareness programs help individuals and organizations stay ahead of evolving cyber threats.



Government agencies and corporate entities have a significant role to play in strengthening cybersecurity frameworks. However, individual responsibility is equally important. By adopting simple cybersecurity practices, we can collectively create a safer digital environment.

Let us work together towards building a secure cyber ecosystem. Remember, cybersecurity is not just an IT issue—it is everyone's responsibility.

A resource person explained Cybersecurity is the practice of protecting systems, networks, and data from cyber threats and attacks. With the increasing reliance on digital platforms, cybersecurity has become a critical aspect of both personal and professional life.

Cybersecurity attacks are malicious attempts to access, damage, disrupt, or steal sensitive data from systems, networks, or devices. Below are some of the most common types of cybersecurity attacks:

1. Phishing Attacks

- Fraudulent emails or messages trick users into revealing sensitive information (e.g., passwords, credit card details).
- Example: A fake email claiming to be from a bank asking for login credentials.

2. Malware Attacks

- Malicious software (viruses, worms, trojans, ransomware) is used to infect systems and steal or destroy data.
- Example: Ransomware encrypts a victim's files and demands a ransom for decryption.

3. Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS) Attacks

- Overloading a network, server, or website with excessive traffic, making it inaccessible to legitimate users.
- Example: Botnets launching a DDoS attack on a company's website.

4. Man-in-the-Middle (MITM) Attacks

- An attacker intercepts communication between two parties to steal or alter information.
- Example: Unsecured public Wi-Fi allowing attackers to eavesdrop on online banking transactions.

5. SQL Injection Attacks

- Exploiting vulnerabilities in web applications to inject malicious SQL queries and gain unauthorized access to databases.
- Example: An attacker retrieves customer data from an e-commerce site's database.

6. Zero-Day Exploits

- Attacks that target software vulnerabilities that are unknown to developers and remain unpatched.
- Example: Exploiting a newly discovered vulnerability in an operating system.

7. Password Attacks

- Attempting to crack passwords using brute-force, dictionary attacks, or credential stuffing.
- Example: Hackers using leaked password databases to gain access to multiple accounts.

8. Insider Threats

- Attacks initiated by employees or individuals with authorized access who misuse their privileges.
- Example: A disgruntled employee leaking confidential company data.

9. Social Engineering Attacks

- Manipulating individuals into revealing confidential information by exploiting human psychology.
- Example: An attacker pretending to be an IT technician and asking for login credentials.

10. Supply Chain Attacks

- Targeting vulnerabilities in third-party vendors or suppliers to infiltrate a larger organization.
- Example: Injecting malware into software updates or compromised hardware.

Best Practices for Cybersecurity:

1. **Use Strong Passwords** – Create complex passwords and enable multi-factor authentication (MFA).
2. **Stay Vigilant Against Phishing** – Verify email sources and avoid clicking on suspicious links.
3. **Keep Software Updated** – Regular updates ensure security patches against vulnerabilities.
4. **Secure Your Network** – Use firewalls, VPNs, and encrypted connections.
5. **Backup Important Data** – Regularly save copies of crucial data to prevent loss.
6. **Use Antivirus and Security Tools** – Employ reliable security software to detect and prevent cyber threats.
7. **Educate and Train Employees** – Awareness programs and simulated attacks can help prevent human errors.
8. **Follow Cybersecurity Regulations** – Adhere to laws and guidelines for data protection and privacy.

Conclusion & Vote of Thanks:

The event successfully increased cybersecurity awareness among participants. The vote of thanks was delivered by Mrs. N. Geethanjali Assistant Professor, Department of CSE – AI & ML. She extended her thanks to the HOD, Principal, and the Management for their support to conduct the workshop and participants for their enthusiastic participation.

Outcomes:

At the end of Presentation, Students will be able to

1. Participants gained knowledge on recognizing and preventing cyber threats.
2. Improved understanding of safe browsing and data protection.
3. Hands-on experience in securing online transactions and digital assets.

The Sustainable Development Goals (SDGs) relevant to the **One Day Training Program on Cybersecurity Awareness** include:

1. **SDG 4: Quality Education** – The workshop provided knowledge and awareness about cybersecurity, equipping students with essential digital skills for a safer online environment.
2. **SDG 9: Industry, Innovation, and Infrastructure** – Promoting cybersecurity awareness supports secure digital infrastructure, which is crucial for sustainable technological development.
3. **SDG 16: Peace, Justice, and Strong Institutions** – Cybersecurity contributes to protecting sensitive information, preventing cybercrimes, and ensuring digital security for individuals and institutions.
4. **SDG 17: Partnerships for the Goals** – Collaboration with experts from DXC Technology enhances knowledge-sharing and strengthens industry-academic partnerships.

Newspaper Clips:



Date : 27/02/2025 EditionName : ANDHRA PRADESH(ANNAMAYYA) PageNo :



ఉత్తమం, వ్యాపారాలు కమ్యూనిటీ సభ్యులను సస్పెండ్ చేయడం ముఖ్య లక్ష్యంగా విద్యార్థులు మెదగాలని ఆయన అన్నారు. డేటా ఉల్లంఘనలకు మానవ తప్పిదం ప్రధాన కారణాలలో ఒకటిగా ఉందని, ఫిషింగ్ దాడులు, రాన్సమ్వేర్ మరియు సోఫిస్టెడ్ ఇంజనీరింగ్ సాఫ్ట్వేలు మరియు అధునాకరణంగా మారాయని ఆయన అన్నారు. ఫిషింగ్ ఇమిటేషన్లు గుర్తించడం, బలపై సాన్సెటివ్ సస్పెండ్లను మరియు పరికరాలను భద్రపరచడంపై విద్యార్థులకు శిక్షణ అందించారు. సైబర్ సెక్యూరిటీ ఇన్ ఫోర్స్ కేవలం ఒకే సమస్య కాదని, ఇవి వ్యాపార అభ్యవసరమని, సైబర్ తెలివితేటలు అభివృద్ధి చెందుతున్నాయన, ఇలాంటి ఛోరస్లు డిజిటల్ యుగంలో సమాచారం ఆక్రమణకర్తగా ఉండటం చాలా అవసరమని, సరైన జ్ఞానం మరియు సాధనాలతో, వ్యక్తులు మరియు సంస్థలు సైబర్ నేరాలకు వ్యతిరేకంగా అటుపొట్లను తప్పిట్లకు గురైనారని, కార్యక్రమంలో కళాశాల చైర్ ప్రెసిడెంట్ పి. రామనాథన్, విభాగాధిపతి డాక్టర్ పద్మ, కే ఆర్ జెన్ డి. గోపాలం, విద్యార్థులు పాల్గొన్నారు.

మరలలలో, మేజర్స్ : మండలంలోని అంగళ్ల పద్మ గల మండపల్లి ఇన్ స్టిట్యూట్ ఆఫ్ టెక్నాలజీ అండ్ సైన్స్ (మిట్స్) కళాశాలలోని కంప్యూటర్ సైన్స్ అండ్ ఇంజనీరింగ్ అప్లిప్లెడ్ ఇంటిలిజెన్స్ మరియు మెషిన్ లెర్నింగ్ విభాగం వారు (పి.ఎం.ఎం) ఆన్లైన్ భద్రత కోసం తాజా సైబర్ తెలివితేటలు మరియు సైబర్ సెక్యూరిటీ ఉత్తమ పథకులపై విద్యార్థులకు బుధవారం అవగాహన కార్యక్రమం నిర్వహించింది. ఈ కార్యక్రమానికి ముఖ్య అతిథిగా కేంద్రంలోని డి.ఎన్.కె.సి విద్యాలయంలో లీడ్ సైబర్ సెక్యూరిటీ ఇంజనీర్ డాక్టర్ పి.గురురాజ్ పాల్గొన్నారు. ఈ కార్యక్రమంలో ఆయన మాట్లాడుతూ ఫిషింగ్ దాడులు, సాన్సెటివ్ నిర్వహణ, సురక్షిత ట్రాజింగ్ అలవాట్లు మరియు డేటా రక్షణ వ్యూహాలు వంటి కీలకమైన అంశాలపై ఆయన విద్యార్థులకు అవగాహన కల్పించారు. సైబర్ దాడుల ప్రమాదాలు పెరుగుతున్నాయన, వ్యక్తులు వారి వ్యక్తీకరణ మరియు వ్యక్తిగత సమాచారం రక్షించుకోవడానికి జ్ఞానాన్ని సమకూర్చుకోవడం అవసరమని, వ్యాపారాలు, వ్యక్తులను లక్ష్యంగా చేసుకుని పెరుగుతున్న సైబర్ దాడులకు, సున్నితమైన డేటాను రక్షించడానికి సైబర్ ప్రమాదాలను ఇంజనీర్ డాక్టర్ పి.గురురాజ్ పాల్గొన్నారు. ఈ కార్యక్రమంలో ఆయన మాట్లాడుతూ ఫిషింగ్ దాడులు, సాన్సెటివ్ నిర్వహణ, సురక్షిత ట్రాజింగ్ అలవాట్లు, డేటా రక్షణ వ్యూహాలు వంటి కీలకమైన అంశాలపై ఆయన విద్యార్థులకు అవగాహన కల్పించారు. సైబర్ దాడుల ప్రమాదాలు పెరుగుతున్నాయన, వ్యక్తులు వారి వ్యక్తీకరణ మరియు వ్యక్తిగత సమాచారం రక్షించుకోవడానికి జ్ఞానాన్ని సమకూర్చుకోవడం అవసరమని, వ్యాపారాలు, వ్యక్తులను లక్ష్యంగా చేసుకుని పెరుగుతున్న సైబర్ దాడులకు, సున్నితమైన డేటాను రక్షించడానికి సైబర్ ప్రమాదాలను ఇంజనీర్ డాక్టర్ పి.గురురాజ్ పాల్గొన్నారు.

