



# MADANAPALLE INSTITUTE OF TECHNOLOGY & SCIENCE

(UGC-AUTONOMOUS INSTITUTION)

Affiliated to JNTUA, Ananthapuramu & Approved by AICTE, New Delhi

NAAC Accredited with A+ Grade

NBA Accredited -B.Tech. (CIVIL, CSE, ECE, EEE, MECH), MBA & MCA



## DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING – AI & ML

### Report on

## One Day Training Program on Cybersecurity Awareness

On

25.02.2025

### Organized by:

Mrs. N. Geethanjali, Assistant Professor, Department of CSE – AI & ML

### Submitted by:

Mrs. N. Geethanjali, Assistant Professor, Department of CSE – AI & ML

### Resource person:

**Dr. Gururaj P-Lead Cybersecurity Engineer, DXC Technology, Bangalore.**

**Participants:** II Year CSE – AI & ML & CSE –Networks – 100 ISTE Student Members

**Venue:** Seminar Hall B

**Mode:** Offline

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

[www.mits.ac.in](http://www.mits.ac.in)

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:

1. **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.
2. **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.
3. **Safe Internet Practices** – Avoid accessing sensitive accounts over public Wi-Fi, ensure software updates are installed regularly, and use secure and legitimate applications.
4. **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.

5. **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.

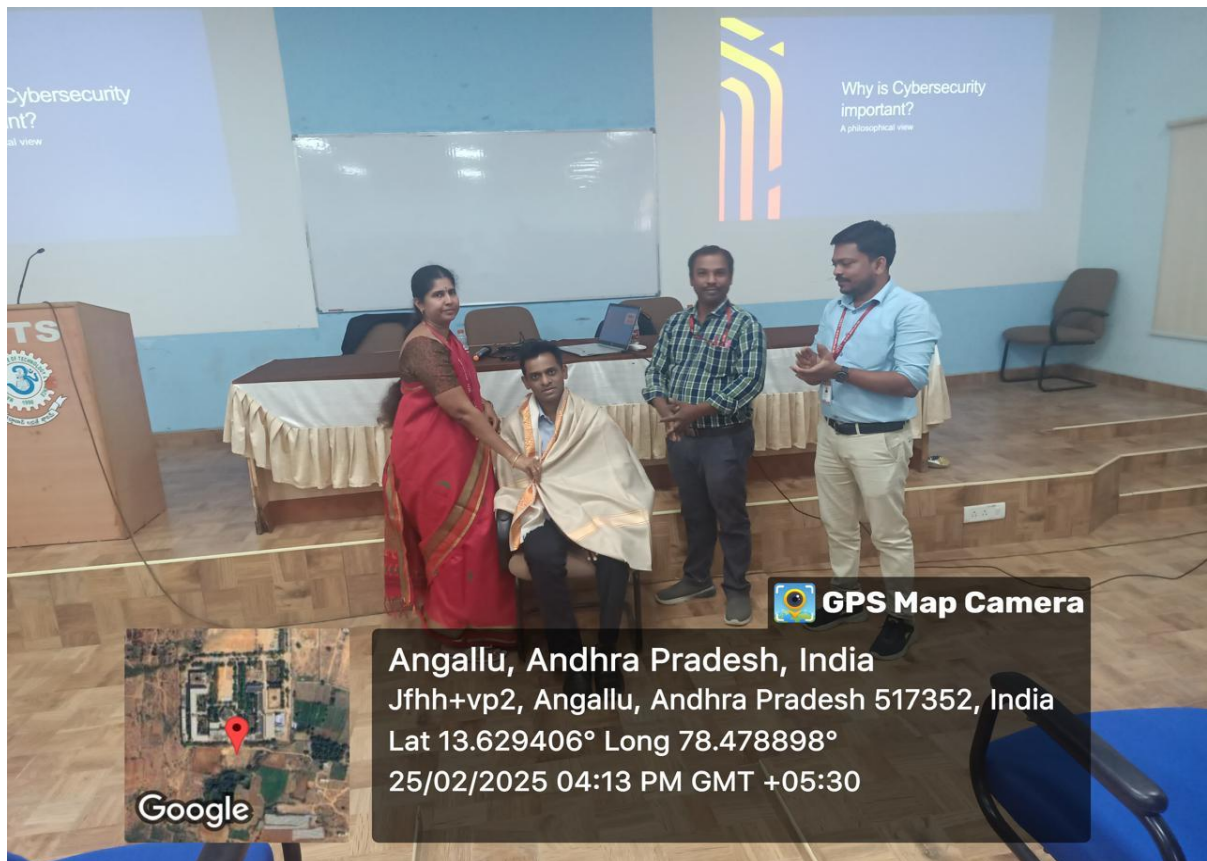


- Example: Injecting malware into software updates or compromised hardware



### 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.

**సైబర్ సెక్యూరిటీపై అవగాహన**



మాట్లాడుతున్న సైబర్ సెక్యూరిటీ ఇంజనీర్ గురురాజ్

మదనపల్లె విద్య. న్యూస్టుడే : సైబర్ సెక్యూరిటీ పద్ధతులపై విద్యార్థులు అవగాహన పెంచుకోవాలని బెంగళూరుకు చెందిన డీఎక్స్ టెక్నాలజీ లీడ్ సైబర్ సెక్యూరిటీ ఇంజనీర్ డాక్టర్ గురు రాజ్ అన్నారు. బుదవారం మిట్స్ ఇంజనీరింగ్ కళాశాలలో కంప్యూటర్ సైన్స్ అండ్ ఇంజనీరింగ్ ఆర్టిఫిషియల్ ఇంటెలిజెన్స్ మెషిన్ లెర్నింగ్ విభాగం ఆధ్వర్యంలో ఆన్లైన్ భద్రత కోసం తాజా సైబర్ బెదిరింపులు, సైబర్ సెక్యూరిటీ ఉత్తమ పద్ధతులపై విద్యార్థులకు అవగాహన కార్యక్రమం నిర్వహించారు. సైబర్ సెక్యూరిటీపై అవగాహన పెంచుకుని రక్షణకోసం సరైన జ్ఞానాన్ని పొందితే సైబర్ దాడులను తప్పిపోవచ్చని తెలిపారు. కార్యక్రమంలో వైస్ ట్రిస్ట్రీ పల్ పి.రామనాథన్, విభాగాధిపతి డాక్టర్ పద్మ, సమన్వయ కర్త గీతాంజలి, విద్యార్థులు పాల్గొన్నారు.

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



**సైబర్ సెక్యూరిటీలో ఉత్తమ పద్ధతులపై మిట్స్ లో అవగాహన కార్యక్రమం**

- హాజరైన డి.ఎక్స్.సి లీడ్ సైబర్ సెక్యూరిటీ ఇంజనీర్ డాక్టర్ పి.గురురాజ్



కురబలకోట, మేజర్ న్యూస్ : మండలంలోని అంగళ్ళు వద్ద గల మదనపల్లె ఇనిస్టిట్యూట్ ఆఫ్ టెక్నాలజీ అండ్ సైన్స్ (మిట్స్) కళాశాలలోని కంప్యూటర్ సైన్స్ అండ్ ఇంజనీరింగ్ ఆర్టిఫిషియల్ ఇంటెలిజెన్స్ మరియు మెషిన్ లెర్నింగ్ విభాగం వారు (ఏబి అండ్ ఎంఎల్) ఆన్లైన్ భద్రత కోసం తాజా సైబర్ బెదిరింపులు మరియు సైబర్ సెక్యూరిటీ ఉత్తమ పద్ధతులపై విద్యార్థులకు బుధవారం అవగాహన కార్యక్రమాన్ని నిర్వహించింది. ఈ కార్యక్రమానికి ముఖ్య అతిథిగా బెంగళూరులోని (డి.ఎక్స్.సి) టెక్నాలజీలో లీడ్ సైబర్ సెక్యూరిటీ ఇంజనీర్ డాక్టర్ పి.గురురాజ్ పాల్గొన్నారు. ఈ కార్యక్ర

మంలో ఆయన మాట్లాడుతూ ఫిషింగ్ దాడులు, పాస్ వర్డ్ నిర్వహణ, సురక్షిత ట్రోజింగ్ అలవాట్లు మరియు డేటా రక్షణ వ్యూహాలు వంటి కీలకమైన అంశాలపై ఆయన విద్యార్థులకు అవగాహన కల్పించారు. సైబర్ దాడుల ప్రమాదాలు పెరుగుతున్నందున, వ్యక్తులు వారి వ్యక్తిగత మరియు వృత్తి పరమైన డేటాను రక్షించుకోవడానికి జ్ఞానాన్ని సమకూర్చడంలో ఇటువంటి వర్క్ షాప్ లు చాలా అవసరమన్నారు. వ్యాపారాలు వ్యక్తులను లక్ష్యంగా చేసుకుని పెరుగుతున్న సైబర్ దాడులకు, సున్నితమైన డేటాను రక్షించడానికి సైబర్ ప్రమాదాలను తగ్గించడానికి అవసరమైన జ్ఞానం సాధనాలతో

ఉద్యోగులు, వ్యాపారాలు కమ్యూనిటీ సభ్యులను సన్నద్ధం చేయడం ముఖ్య లక్ష్యంగా విద్యార్థులు మెదగాలని ఆయన అన్నారు. డేటా ఉల్లంఘనలకు మానవ తప్పిదం ప్రధాన కారణాలలో ఒకటిగా ఉందని, ఫిషింగ్ దాడులు, రాన్సమ్ వేర్ మరియు సోషల్ ఇంజనీరింగ్ స్కామ్ లు మరింత అధునాతనంగా మారాయని ఆయన అన్నారు. ఫిషింగ్ ఇమెయిల్ లను గుర్తించడం, బలమైన పాస్ వర్డ్ లను సృష్టించడం మరియు పరికరాలను భద్రపరచడంపై విద్యార్థులకు శిక్షణ అందించారు. సైబర్ సెక్యూరిటీ ఇకపై కేవలం ఐటీ సమస్య కాదని, ఇది వ్యాపార అత్యవసరమని, సైబర్ బెదిరింపులు అభివృద్ధి చెందుతున్నందున, ఇలాంటి చొరవలు డిజిటల్ యుగంలో సమాచారం అప్రమత్తంగా ఉండటం చాలా అవసరమని, సరైన జ్ఞానం మరియు సాధనాలతో, వ్యక్తులు మరియు సంస్థలు సైబర్ నేరాలకు వ్యతిరేకంగా అటుపోట్లను తిప్పికొట్టగలవన్నారు. ఈ కార్యక్రమంలో కళాశాల వైస్ ట్రిస్ట్రీ పాల్ పి.రామనాథన్, విభాగాధిపతి డాక్టర్ పద్మకో - ఆర్డినేటర్ గీతాంజలి, విద్యార్థులు పాల్గొన్నారు.

# మిట్స్ కళాశాల లో ఆన్లైన్ భద్రత సైబర్ సెక్యూరిటీ పై విద్యార్థులకు అవగాహన



**మదనపల్లి ఫిబ్రవరి 26, ( వి. శ్రీనివాసులు రెడ్డి తరణం విలేజ్ )** :మదనపల్లి సమీపంలోని మదనపల్లి ఇన్స్టిట్యూట్ ఆఫ్ టెక్నాలజీ అండ్ సైన్స్ (మిట్స్) కలశాలలోని కంప్యూటర్ సైన్స్ అండ్ ఇంజనీరింగ్ ఆర్టిఫిషియల్ ఇంటెలిజెన్స్ మెషిన్ లెర్నింగ్ విభాగం వారు ఆన్లైన్ భద్రత కోసం తాజా సైబర్ బెదిరింపులు మరియు సైబర్ సెక్యూరిటీ ఉత్తమ పద్ధతులపై విద్యార్థులకు అవగాహన కార్యక్రమాన్ని నిర్వహించారు. ఈ కార్యక్రమానికి ముఖ్య అతిథిగా బెంగళూరులోని డి.ఎక్స్.సి టెక్నాలజీలో లీడ్ సైబర్ సెక్యూరిటీ ఇంజనీర్ డాక్టర్ పి. గురురాజ్ హాజరయ్యారు. ఈ సందర్భంగా ఆయన మాట్లాడుతూ ఫిషింగ్ దాడులు, పాస్వర్డ్ నిర్వహణ, సురక్షిత బ్రౌజింగ్ అలవాట్లు మరియు డేటా రక్షణ పూర్వోలు వంటి కీలకమైన అంశాల పై ఆయన విద్యార్థులకు అవగాహన కల్పించారు. సైబర్ దాడుల ప్రమాదాలు పెరుగుతున్నందున, వ్యక్తులు వారి వ్యక్తిగత మరియు వృత్తిపరమైన డేటాను రక్షించుకోవడానికి జానాన్ని సమకూర్చడంలో ఇటువంటి వర్క్‌షాప్‌లు చాలా అవసరమని పేర్కొన్నారు. వ్యాపారాలు మరియు వ్యక్తులను లక్ష్యంగా చేసుకుని పెరుగుతున్న సైబర్

దాడులకు, సున్నితమైన డేటాను రక్షించడానికి మరియు సైబర్ ప్రమాదాలను తగ్గించడానికి అవసరమైన జ్ఞానం మరియు సాధనాలతో ఉద్యోగులు, వ్యాపారాలు మరియు కమ్యూనిటీ సభ్యులను సన్నద్ధం చేయడం ముఖ్య లక్ష్యం గా విద్యార్థులు యెదగాలన్నారు. డేటా ఉల్లంఘనలకు మానవ తప్పిదం ప్రధాన కారణాలలో ఒకటిగా ఉందని, ఫిషింగ్ దాడులు, రాన్సమ్వేర్ మరియు సోషల్ ఇంజనీరింగ్ స్కామ్‌లు మరింత అధునాతనంగా మారాయిన్నారు. ఫిషింగ్ ఇమెయిల్‌లను గుర్తించడం, బలమైన పాస్వర్డ్‌లను సృష్టించడం మరియు పరికరాలను భద్రపరచడంపై విద్యార్థులకు శిక్షణ అందించారు. సైబర్ సెక్యూరిటీ ఇకపై కేవలం ఐటీ సమస్య కాదని, ఇది వ్యాపార అభ్యవసరం అని, సైబర్ బెదిరింపులు అభివృద్ధి చెందు తున్నందున, ఇలాంటి చొరవలు డిజిటల్ యుగంలో సమాచారం మరియు అప్రమత్తంగా ఉండటం చాలా అవసరమని, సరైన జ్ఞానం మరియు సాధనాలతో, వ్యక్తులు మరియు సంస్థలు సైబర్ నేరాలకు వ్యతిరేకంగా ఆటుపోట్లను తిప్పికొట్టగలవని అన్నారు. ఈ కార్యక్రమం లో కళాశాల వైస్ ప్రెసిడెంట్ పి. రామనాథన్, విభాగాధిపతి డాక్టర్ పద్మ, కో ఆర్డినేటర్ గీతాంజలి, విద్యార్థులు పాల్గొన్నారు.



## ఆన్లైన్ భద్రత కోసం తాజా సైబర్ బెదిరింపులు

సైబర్ సెక్యూరిటీ ఉత్తమ పద్ధతులపై...

మిట్స్ కళాశాల విద్యార్థులకు అవగాహన సదస్సు..

ముఖ్య అతిథిగా హాజరైన సైబర్ సెక్యూరిటీ ఇంజనీర్ డాక్టర్ గురురాజ్..

**మదనపల్లి (నిహా సూర్య)**  
మదనపల్లి ఇన్స్టిట్యూట్ ఆఫ్ టెక్నాలజీ, సైన్స్ (మిట్స్) కలశాలలోని కంప్యూటర్ సైన్స్, ఇంజనీరింగ్ ఆర్టిఫిషియల్ ఇంటెలిజెన్స్ మెషిన్ లెర్నింగ్ విభాగం వారు (ఏబి, ఎం ఎల్ ) ఆన్లైన్ భద్రత కోసం తాజా సైబర్ బెదిరింపులు, సైబర్ సెక్యూరిటీ ఉత్తమ పద్ధతులపై విద్యార్థులకు అవగాహన కార్యక్రమాన్ని నిర్వహించారు.. ఈ కార్యక్రమానికి ముఖ్య అతిథిగా బెంగళూరులోని డి ఎక్స్ సి టెక్నాలజీలో లీడ్ సైబర్ సెక్యూరిటీ ఇంజనీర్ డాక్టర్ గురురాజ్. పి పాల్గొన్నారు. కార్యక్రమంలో ఫిషింగ్ దాడులు, పాస్వర్డ్ నిర్వహణ, సురక్షిత బ్రౌజింగ్ అలవాట్లు, డేటా రక్షణ పూర్వోలు వంటి కీలకమైన అంశాల పై ఆయన విద్యార్థులకు అవగాహన కల్పించారు. సైబర్ దాడుల ప్రమాదాలు పెరుగుతున్నందున, వ్యక్తులు వారి వ్యక్తిగత,వృత్తిపరమైన డేటాను రక్షించుకోవడానికి జానాన్ని సమకూర్చడంలో ఇటువంటి వర్క్‌షాప్‌లు చాలా అవసరమన్నారు. వ్యాపారాలు,వ్యక్తులను లక్ష్యంగా చేసుకుని పెరుగుతున్న సైబర్ దాడులకు, సున్నితమైన డేటాను రక్షించడానికి, సైబర్ ప్రమాదాలను తగ్గించడానికి అవసరమైన జ్ఞానం, సాధనాలతో ఉద్యోగులు, వ్యాపారాలు,కమ్యూనిటీ సభ్యులను సన్నద్ధం చేయడం ముఖ్య లక్ష్యంగా విద్యార్థులు మెలగాలని సూచించారు. డేటా ఉల్లంఘనలకు మానవ తప్పిదం ప్రధాన కారణాలలో ఒకటిగా ఉందని, ఫిషింగ్ దాడులు, రాన్సమ్వేర్,సోషల్ ఇంజనీరింగ్ స్కామ్‌లు మరింత అధునాతనంగా మారాయన్నారు. ఫిషింగ్ ఇమెయిల్‌లను గుర్తించడం, బలమైన పాస్వర్డ్‌లను సృష్టించడం,



పరికరాలను భద్రపరచడంపై విద్యార్థులకు శిక్షణ అందించారు. సైబర్ సెక్యూరిటీ ఇకపై కేవలం ఐటీ సమస్య కాదని, ఇది వ్యాపార అభ్యవసరమని చెప్పారు. సైబర్ బెదిరింపులు అభివృద్ధి చెందుతున్నందున, ఇలాంటి చొరవలు డిజిటల్ యుగంలో సమాచారం, అప్రమత్తంగా ఉండటం చాలా అవసరమని తెలియజేశారు. సరైన జ్ఞానం,సాధనాలతో, వ్యక్తులు, సంస్థలు సైబర్ నేరాలకు వ్యతిరేకంగా ఆటుపోట్లను తిప్పికొట్టగలవన్నారు. కార్యక్రమంలో కళాశాల వైస్ ప్రెసిడెంట్ పి. రామనాథన్, విభాగాధిపతి డాక్టర్ పద్మ, కో ఆర్డినేటర్ గీతాంజలి, విద్యార్థులు పాల్గొన్నారు.

## **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.
4. Encouragement to follow cybersecurity best practices in daily digital activities.

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.