Dr.Mahalingam College of Engineering and Technology, Pollachi-642003
Teaching Learning Centre
Report on Faculty Development Program on "Cyber Security"

Date: 27.05.2024 10 31.05.2024
Venue : Mechanical Department Conference Hall
Host : Teaching Learning Centre

Introduction

The Faculty Development Program (FDP) on Cyber Security was conducted from 27.05.2024 to 31.05.2024, aimed at enhancing the knowledge and skills of faculty members in the field of cyber security. Furthermore, it was designed to provide an in-depth understanding of various aspects of cyber security, including cybercrime, cyber laws, social media security, e-commerce, digital payments, and security for digital devices. The program covered a wide range of topics essential for understanding and mitigating cyber threats, ensuring safe practices in digital environments.

27.05.2024 – Day 1: Introduction to Cyber Security

Mrs. S.C. Lavanya, Assistant Professor (SS), Department of Computer Science and Engineering (CSE), delivered a session on "Introduction to Cyber Security." And rendered the following points:

- Overview: The session began with a comprehensive overview of cyber security, highlighting its importance in today's digital world.
- Key Concepts: Participants were introduced to fundamental concepts, including threat vectors, risk management, and security protocols.
- Importance: Emphasis was placed on the critical need for robust cyber security measures to protect sensitive information and maintain privacy.

Fig.1

28.05.2024 – Day 2: Cyber crime and Cyber law

Mr. M. Sakthivadivel, Assistant Professor (SS), Department of Cyber Security, presented an enlightening session on Cyber Crime and Cyber Law, providing participants with a deep understanding of the legal frameworks and real-world implications of cyber threats.

- **Cyber Crime**: This segment covered various types of cyber-crimes, such as hacking, phishing, identity theft, and ransom ware attacks.

- **Case Studies**: Real-world examples of cybercrimes were discussed to illustrate the impact and methodologies of attackers.

Fig.2

29.05.2024 – Day 3: Social Media Overview and Security

Mr. M. Sakthivadivel, Assistant Professor (SS), Department of Cyber Security, presented an informative session on "Social Media Overview and Security."

- **Social Media Risks**: The session addressed the security risks associated with social media platforms, including data breaches, fake profiles, and privacy concerns.

- **Best Practices**: Guidelines for maintaining security on social media were provided, such as using strong passwords, enabling two-factor authentication, and being cautious about sharing personal information.

- **Tools**: Tools and techniques to monitor and secure social media accounts were discussed.

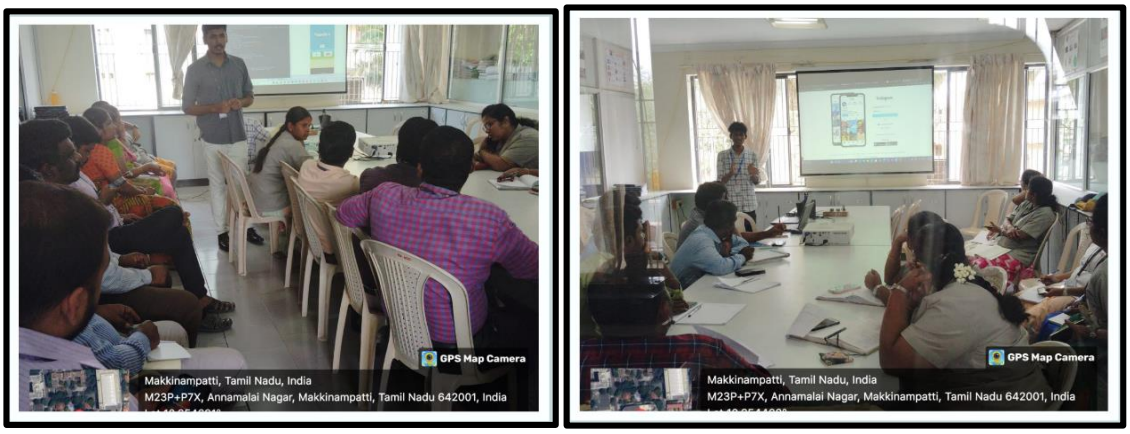

Fig.3

30.05.2024 – Day 4: E-Commerce and Digital Payments

Ms. K. Radha, Assistant Professor, Department of Computer Science and Engineering (CSE), rendered a thought provoking session on "E-Commerce and Digital Payments."

- **E-Commerce Security**: The focus was on securing e-commerce platforms, including safeguarding customer data, securing payment gateways, and preventing fraud.

- **Digital Payment Security**: Security measures for digital payments were discussed, including encryption, secure authentication methods, and compliance with standards like PCI DSS.

- **Best Practices**: Tips for safe online transactions, such as recognizing phishing attempts and using secure payment methods, were shared.

Fig.4

31.05.2024 – Day 5: Digital Devices Security, Tools and Technologies for Cyber Security

Ms. K. Saranya, Assistant Professor, Department of Information Technology, delivered a session focusing on Digital Devices Security, Tools, and Technologies for Cyber Security.

- **Security Tools**: Participants were introduced to various tools and technologies used in cyber security, such as firewalls, intrusion detection systems, and SIEM (Security Information and Event Management) systems.
- **Hands-On Training**: Practical sessions were conducted to familiarize participants with the use of these tools.
- **Emerging Technologies**: The role of emerging technologies like artificial intelligence and machine learning in enhancing cyber security was explored.

Fig.5

Feedback and Outcomes

The FDP received positive feedback from participants, who appreciated the detailed coverage of topics and the practical insights provided. Key outcomes included:

- Improved understanding of cyber security fundamentals and the latest trends.
- Enhanced ability to identify and respond to cyber threats.
- Increased awareness of legal aspects related to cyber security.
- Practical knowledge of tools and technologies for securing digital environments.

Valedictory Note

From this Faculty Development Program on Cyber Security, it is evident that the knowledge gained over the past week will empower each participant to contribute effectively to their institutions and communities. Cyber security is not just a technical necessity but a crucial aspect of safeguarding our digital identities and organizational assets in an increasingly interconnected world.

Dr. P. Govindasamy, Principal has distributed the certificates and appreciation note to the invited speakers and the participants.

Conclusion

The Faculty Development Program on Cyber Security was successful in achieving its objectives of educating and empowering faculty members with the knowledge and skills necessary to tackle cyber threats. The comprehensive coverage of topics ensured that participants are well-equipped to implement and teach cyber security best practices.