Gyanmanjari Institute of Technology Bhavnagar

Report on

An Expert Talk on

Cyber Security Awareness

Date: 05/08/2024
Time: 01:30 PM
Venue: Seminar Hall (GF-28)

No. of Student	86
Department	Degree - Information Technology
Semester	5th – (B-2022)
Faculty Co-Ordinator	Prof. Sunil H. Chavda

About Expert:

Mr. Narasimha Rao, Mr. Ishan Gupta, Mr. Dhruvrajsinh Jadeja and Mr. Gopal Rathod

Organisation: Cyber Cell Bhavnagar.

Objective of Talk

- Introduction to Cyber Security
- Case Study: Cyber – Attack using Physical Profile
- Data Collection Strategies of Cyber Attack
- Protection again Hacking and Its different Techniques
- Q&A Session

About Expert Session

- **Introduction to Cyber Security**

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These attacks often aim to access, change, or destroy sensitive information; extort money from users; or disrupt normal business operations. Effective cybersecurity requires a multi-layered approach, including robust defences, user education, and proactive threat detection to safeguard digital assets and ensure data integrity.

- **Case Study: Cyber – Attack using Physical Profile**

A high-profile cyber-attack exploited a physical profile by using an infected USB drive left in a public space. An employee unknowingly plugged it into a company computer, enabling malware to infiltrate the network. This breach compromised sensitive data and highlighted the critical need for stringent physical security measures and employee awareness training in cybersecurity protocols.

- **Data Collection Strategies of Cyber Attack**

Cyber attackers employ various data collection strategies to gather sensitive information. Phishing scams trick users into revealing personal data through deceptive emails or websites. Malware, such as keyloggers and spyware, silently monitors and captures keystrokes and activities. Man-in-the-middle attacks intercept and manipulate communication between two parties. Social engineering exploits human psychology to extract confidential information. Additionally, exploiting vulnerabilities in software and hardware allows attackers to gain unauthorized access to databases and systems, compromising data security.

- **Protection again Hacking and Its different Techniques**

Protecting against hacking requires a multi-faceted approach. Implement strong, unique passwords and enable multi-factor authentication. Regularly update and patch software to fix vulnerabilities. Use firewalls and antivirus programs to detect and block threats. Encrypt sensitive data to protect it from unauthorized access. Educate users on recognizing phishing scams and social engineering tactics. Conduct regular security audits and penetration testing to identify and mitigate risks. Employ intrusion detection systems to monitor network activity and respond swiftly to potential threats.

- **Q&A Session**

During the Q&A session, attendees can ask specific questions about cybersecurity practices, recent cyber-attack case studies, data protection strategies, and the latest hacking techniques. Experts will provide detailed answers, share insights, and recommend best practices to enhance security and prevent cyber threats effectively.

Photographs