Mahatma Phule Shikshan Sanstha's

Karmaveer Bhaurao Patil College, Urun-Islampur,

Taluka - Walwa, Dist - Sangli

Department of BCS

Academic Year 2024 - 25

Report On

Guest Lecture

" Cyber Security & Social Media "

Introduction:

On 20th February, 2025 a guest lecture on "Cyber Security and Social Media" was delivered by Adv. Rajvardhini Bhosale. The lecture explored the growing intersection of cyber security challenges and social media platforms, focusing on how social media has become a significant vector for cyber threats and the importance of maintaining digital security. The session provided insights into practical measures for protecting personal and organizational data in the increasingly interconnected online world.

Key Points Discussed:

1. **Cyber security Threats in Social Media:** The speaker opened the discussion by highlighting the various cyber security risks associated with social media platforms. These threats include:

- **Phishing Attacks:** Malicious actors often use social media to impersonate legitimate individuals or organizations, tricking users into sharing sensitive information or clicking on harmful links.
- **Data Breaches:** Social media platforms store vast amounts of personal data, which, if compromised, can lead to identity theft, financial fraud, and other malicious activities.
- **Malware and Ransomware:** Cybercriminals may use social media as a means to distribute malware or ransomware, either through infected links or by exploiting vulnerabilities in the platform itself.

- **Social Engineering:** Attackers leverage information from users' profiles, posts, and connections to manipulate individuals into disclosing confidential information or granting unauthorized access.

2. **Impact on Privacy:** Social media platforms have access to enormous quantities of user data. The speaker discussed how this data can be exploited, particularly by third-party advertisers or malicious actors. A few important privacy concerns mentioned were:

- **User Profiling:** Social media companies collect and analyse user data to create detailed profiles for targeted advertising. This raises questions about the extent of privacy violations and user consent.
- **Data Retention:** Despite a user's attempts to delete or deactivate an account, much of the data remains stored in the platform's databases, posing long-term privacy risks.
- **Location Tracking:** Many platforms track users' real-time locations through their mobile devices, which can be used for both marketing purposes and more malicious activities if exposed to cybercriminals.

3. **Social Media and Psychological Manipulation:** Another significant topic discussed was how social media platforms can influence behaviour and decision-making through cyber means:

- **Fake News and Misinformation:** Cyber security threats extend beyond technical attacks to include psychological tactics, such as the spread of fake news or misinformation. This can lead to social unrest, political instability, and other far-reaching consequences.
- **Influence Campaigns:** Cybercriminals or malicious actors, including state-sponsored groups, can exploit social media for political manipulation or to create divisions within society by amplifying divisive messages.

4. **Protecting Against Cyber Threats on Social Media:** The speaker provided practical advice on how to safeguard against these risks, including:

- **Strong Passwords and Two-Factor Authentication (2FA):** One of the easiest and most effective measures to prevent unauthorized access to social media accounts is by using strong, unique passwords and enabling 2FA for an added layer of protection.
- **Privacy Settings:** Social media platforms offer various privacy settings that allow users to control who can see their posts, send them messages, or access their personal information. Regularly reviewing and updating privacy settings can significantly reduce exposure to potential cyber threats.
- **Awareness and Education:** Users need to stay informed about the latest threats and scams. Social media platforms and cyber security experts emphasize the importance of recognizing suspicious behaviour or phishing attempts and reporting them to the platform administrators.
- **Regular Software Updates:** Ensuring that social media apps and associated devices are kept up to date with the latest security patches helps to minimize vulnerabilities that can be exploited by attackers.

5. **Legal and Ethical Implications:** The lecture also touched upon the legal responsibilities of social media companies and individuals in maintaining cyber security:

- **Data Protection Laws:** Several international regulations, such as the General Data Protection Regulation (GDPR), govern how user data is collected, stored, and shared by social media platforms. The speaker discussed how these laws aim to protect user privacy and prevent misuse.
- **Responsibility of Social Media Platforms:** The ethical responsibility of platforms to secure user data and detect and prevent cyber threats was debated. There is increasing pressure on companies to invest in cyber security infrastructure and take proactive steps to secure user information.

Conclusion:

The guest lecture on cyber security and social media emphasized the critical need for vigilance in protecting personal and organizational data in the digital age. With the growing reliance on social media for both personal and professional purposes, understanding the risks and adopting proactive security measures is essential. The lecture reinforced the idea that cyber security is not just the responsibility of organizations and governments, but also of individuals who must stay informed and adopt best practices to safeguard their online presence.

Photographs :

Felicited of guest by principal Dr. N.S. Shinde

Dr. Promod Ganganmale gave welcome speech

Dr. B. A. Sawant gave introduction to guest

Presidential speech gave by principal Dr. N. S. Shinde

Students

Mr. P. M. More gave Vote of Thanks

Head of BCS Department