

SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (Common to Department of CSE and Cyber Security)

QUESTION BANK



VII SEMESTER OCY102-Social Media Security Regulation – 2023

Academic Year 2026-2027 (Odd- Semester)

Prepared by

Ms. V. Vijay Priya Assistant Professor(O.G)/CSE

Ms.D.Keerthivasan , Assistant Professor(O.G)/CSE

Ms.T.Sathya, Assistant Professor (O.G)/Cyber Security



SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
& DEPARTMENT OF CYBER SECURITY

QUESTION BANK



SUBJECT: OCY102 SOCIAL MEDIA SECURITY

SEM / YEAR: VII / IV

UNIT I – INTRODUCTION TO SOCIAL MEDIA SECURITY

Social Media Platforms-Communication Impact- Cyber security Basics- Security Threats User Awareness- Breach Case Studies-Data Collection- Security Features- Future Trends

PART-A

Q.No.	Questions	BT Level	Competence
1	Define social media platforms.	BTL1	Remembering
2	List any four examples of social media platforms.	BTL1	Remembering
3	State any two advantages of social media communication.	BTL2	Understanding
4	Mention any two disadvantages of social media communication.	BTL2	Understanding
5	What is meant by communication impact in social media?	BTL1	Remembering
6	Define cyber security.	BTL1	Remembering
7	What are the three principles of the CIA triad?	BTL1	Remembering
8	Define confidentiality in cyber security.	BTL1	Remembering
9	What is integrity in information security?	BTL1	Remembering
10	What is availability in cyber security?	BTL1	Remembering
11	Explain malware with an example.	BTL2	Understanding
12	What is phishing?	BTL1	Remembering
13	What is ransomware?	BTL1	Remembering
14	Define social engineering attack.	BTL1	Remembering
15	What is a data breach?	BTL1	Remembering
16	Explain user awareness in cyber security?	BTL2	Understanding
17	List any two security features available in social media platforms.	BTL1	Remembering
18	What is Two-Factor Authentication (2FA)?	BTL1	Remembering
19	What is end-to-end encryption?	BTL1	Remembering
20	Mention any two future trends in cyber security.	BTL1	Remembering

21	What is Artificial Intelligence in cyber security?	BTL1	Remembering	
22	Differentiate between malware and ransomware.	BTL2	Understanding	
23	Explain the role of privacy settings in social media security.	BTL2	Understanding	
24	Differentiate between authentication and authorization.	BTL2	Understanding	
	PART-B			
Q.No.	Questions	Marks	BT Level	Competence
1	Illustrate various social media platforms and discuss their features, applications, and benefits.	(16)	BTL3	Applying
2	Discuss the impact of social media on communication with suitable examples.	(16)	BTL4	Analyzing
3	Discuss the Various fundamentals of cyber security and describe the CIA triad in detail.	(16)	BTL4	Analyzing
4	Describe various cyber security threats and their effects on individuals and organizations.	(16)	BTL3	Applying
5	Illustrate phishing, malware, ransomware, and social engineering attacks with suitable examples.	(16)	BTL3	Applying
6	Describe the importance of user awareness and suggest preventive measures against cyber-attacks.	(16)	BTL3	Applying
7	Analyze major data breach case studies and discuss the lessons learned from them.	(16)	BTL4	Analyzing
8	Analyze how social media platforms collect user data and discuss privacy issues associated with data collection.	(16)	BTL4	Analyzing
9	Discuss the various security features provided by modern social media platforms.	(16)	BTL3	Applying
10	Evaluate the effectiveness of authentication mechanisms such as passwords, biometrics, and 2FA.	(16)	BTL5	Evaluating
11	Analyze the role of encryption in securing online communication and user data.	(16)	BTL4	Analyzing
12	Evaluate the impact of social media on privacy and cyber security.	(16)	BTL5	Evaluating
13	Describe Various future trends in cyber security including Artificial Intelligence, Blockchain, and Zero Trust Security.	(16)	BTL3	Applying
14	Evaluate emerging cyber security technologies for protecting social media users.	(16)	BTL5	Evaluating
15	Design a cyber security awareness program for social media users to minimize security threats.	(16)	BTL6	Creating
16	Develop an awareness campaign to educate users about phishing and social engineering attacks.	(16)	BTL6	Creating
17	Assess the impact of data collection practices on user privacy and security.	(16)	BTL5	Evaluating

UNIT II- PRIVACY AND ACCOUNT SECURITY

Privacy Settings-Strong Passwords-Two-Factor Authentication (2FA)- Geotagging Risks Personal Information-Third-Party Apps-Account Takeover-Encryption RoleSafe Posting.

PART-A			
Q.No.	Questions	BT Level	Competence
1	What are privacy settings in social media platforms?	BTL1	Remembering
2	List any two benefits of using privacy settings.	BTL1	Remembering
3	State two advantages of enabling 2FA.	BTL2	Understanding
4	Define a strong password.	BTL1	Remembering
5	Mention any two risks associated with geotagging.	BTL2	Understanding
6	Explain the importance of reviewing app permissions before installing third-party applications.	BTL2	Understanding
7	Mention any two characteristics of a strong password.	BTL1	Remembering
8	How can third-party applications affect user privacy?	BTL2	Understanding
9	How do privacy settings contribute to online security?	BTL2	Understanding
10	What is Two-Factor Authentication (2FA)?	BTL1	Remembering
11	Explain the importance of protecting personal information online.	BTL2	Understanding
12	What is geotagging?	BTL1	Remembering
13	What is meant by personal information in social media?	BTL1	Remembering
14	What precautions should be taken before installing third-party applications?	BTL2	Understanding
15	How does 2FA help prevent account takeover?	BTL2	Understanding
16	Give two examples of sensitive personal information.	BTL1	Remembering
17	What are third-party applications?	BTL1	Remembering
18	Explain why sharing location information online can be risky.	BTL2	Understanding
19	Differentiate between weak passwords and strong passwords.	BTL2	Understanding
20	What is safe posting on social media?	BTL1	Remembering
21	State the role of encryption in cyber security.	BTL2	Understanding
22	Define account takeover.	BTL1	Remembering
23	List any two causes of account takeover attacks.	BTL1	Remembering
24	What is encryption?	BTL1	Remembering

PART-B				
Q.No.	Questions	Marks	BT Level	Competence
1	Illustrate the importance of privacy settings in social media platforms and discuss how they protect user information.	(16)	BTL3	Applying
2	Discuss the characteristics of strong passwords and explain best practices for password management.	(16)	BTL4	Analyzing
3	Describe the working principle of Two-Factor Authentication (2FA) and discuss its advantages in securing online accounts.	(16)	BTL3	Applying
4	Analyze the risks associated with geotagging and suggest preventive measures to protect user privacy.	(16)	BTL4	Analyzing
5	Discuss the importance of protecting personal information on social media platforms with suitable examples.	(16)	BTL4	Analyzing
6	Analyze the role of third-party applications in social media and analyze the security risks associated with them.	(16)	BTL4	Analyzing
7	Describe account takeover attacks, their causes, consequences, and prevention techniques.	(16)	BTL3	Applying
8	Analyze the role of encryption in securing online communication and protecting user data.	(16)	BTL4	Analyzing
9	Discuss safe posting practices on social media and explain how they help maintain privacy and security.	(16)	BTL4	Analyzing
10	Analyze the effectiveness of privacy settings and Two-Factor Authentication in protecting social media accounts.	(16)	BTL4	Analyzing
11	Evaluate different password protection techniques and recommend the best strategy for securing user accounts.	(16)	BTL5	Evaluating
12	Assess the impact of sharing personal information and location data on social media platforms.	(16)	BTL5	Evaluating
13	Evaluate the security risks posed by third-party applications and propose suitable mitigation strategies.	(16)	BTL5	Evaluating
14	Design a security awareness program to educate users about safe social media practices.	(16)	BTL6	Creating
15	Evaluate the effectiveness of encryption and 2FA in preventing cyber attacks on social media platforms.	(16)	BTL5	Evaluating
16	Develop a comprehensive strategy to protect social media users from account takeover attacks and privacy breaches.	(16)	BTL6	Creating
17	Assess the privacy implications of geo tagging and location sharing features in modern applications.	(16)	BTL5	Evaluating
UNIT III- THREATS AND ATTACKS				
Social Engineering-Cybercriminal Tactics-Suspicious Activity-Malware Links- Hacking Cases-Suspicious Content-Security Tests-Insider Threats- Threat Intelligence.				
PART-A				
Q.No.	Questions		BT Level	Competence

1	Define Social Engineering.	BTL1	Remembering
2	List any four types of Social Engineering attacks.	BTL1	Remembering
3	What is Suspicious Activity in social media platforms?	BTL1	Remembering
4	What is phishing? How does it differ from spear phishing?	BTL1	Remembering
5	Define Cybercriminal Tactics with examples.	BTL1	Remembering
6	What are malware links?	BTL1	Remembering
7	List four indicators of suspicious online activity.	BTL1	Remembering
8	Define hacking. Differentiate ethical and malicious hacking.	BTL1	Remembering
9	Define Malware. Mention four types.	BTL1	Remembering
10	Differentiate Insider and External Threats.	BTL2	Understanding
11	Explain the Best practices for protecting social media accounts.	BTL2	Understanding
12	What is Suspicious Content?	BTL1	Remembering
13	What are Security Tests?	BTL1	Remembering
14	Define Insider Threats.	BTL1	Remembering
15	What is Threat Intelligence?	BTL1	Remembering
16	Explain Role of CTI in incident response.	BTL2	Understanding
17	List types of Threat Intelligence.	BTL1	Remembering
18	Define VAPT.	BTL1	Remembering
19	What is clickjacking?	BTL1	Remembering
20	Explain Preventive measures against social engineering.	BTL2	Understanding
21	Differentiate virus, worm and Trojan.	BTL2	Understanding
22	What is a data breach?	BTL1	Remembering
23	What is ransomware?	BTL1	Remembering
24	List the Objectives of security testing.	BTL1	Remembering

PART-B

Q.No.	Questions	Marks	BT Level	Competence
1	Discuss the concept of Social Engineering and discuss various social engineering attacks such as phishing, baiting, pretexting, and tailgating with suitable examples.	(16)	BTL3	Applying
2	Analyze the different Cybercriminal Tactics used in modern cyber attacks and explain their impact on individuals and organizations.	(16)	BTL4	Analyzing
3	Discuss various types of Suspicious Activities in computer networks and explain methods used to detect and respond to them.	(16)	BTL3	Applying

4	Analyze the dangers of Malware Links and describe techniques used to identify and prevent malware infections.	(16)	BTL4	Analyzing
5	Examine major Hacking Cases and analyze the causes, attack methods, and lessons learned from these incidents.	(16)	BTL4	Analyzing
6	Describe the characteristics of Suspicious Content in emails, websites, and social media messages and explain methods for identifying such content.	(16)	BTL3	Applying
7	Analyze the importance of Security Testing and discuss various testing methods such as vulnerability assessment, penetration testing, and security auditing.	(16)	BTL4	Analyzing
8	Analyze the causes and consequences of Insider Threats and propose effective mitigation strategies for organizations.	(16)	BTL4	Analyzing
9	Evaluate the process of Threat Intelligence collection, analysis, and dissemination in cyber security operations.	(16)	BTL5	Evaluating
10	Evaluate the role of Threat Intelligence in detecting and preventing advanced cyber attacks in organizations.	(16)	BTL5	Evaluating
11	Compare different Social Engineering Techniques and evaluate their effectiveness in compromising security systems.	(16)	BTL5	Evaluating
12	Design an awareness program to educate employees about Cybercriminal Tactics, Malware Links, and Suspicious Content.	(16)	BTL6	Creating
13	Develop a comprehensive security strategy to reduce the risks associated with Insider Threats in an organization.	(16)	BTL6	Creating
14	Evaluate the effectiveness of different Security Testing Techniques in protecting enterprise networks from cyber attacks.	(16)	BTL5	Evaluating
15	Create a framework for integrating Threat Intelligence into an organization's cyber security incident response process.	(16)	BTL6	Creating
16	Analyze the lifecycle of a social engineering attack and discuss preventive measures to reduce human-related security risks.	(16)	BTL4	Analyzing
17	Analyze the role of vulnerability assessment and penetration testing in security testing.	(16)	BTL4	Analyzing

UNIT IV- LEGAL AND ETHICAL ISSUES

International Laws-Intellectual Property-Privacy Policies-Ethical Data Use- User Responsibilities-Legal Disputes- Freedom of Speech-Compliance Requirements Regulation Future.

PART-A

Q.No.	Questions	BT Level	Competence
1	Define Cyber Law.	BTL1	Remembering
2	What are International Cyber Laws?	BTL1	Remembering
3	Define Intellectual Property (IP).	BTL1	Remembering
4	Differentiate between Copyright and Patent.	BTL2	Understanding

5	What is a Privacy Policy?	BTL1	Remembering
6	State four objectives of a Privacy Policy.	BTL1	Remembering
7	What is Ethical Data Use?	BTL1	Remembering
8	List four ethical principles governing social media usage.	BTL1	Remembering
9	What are User Responsibilities in social media?	BTL1	Remembering
10	Define Legal Dispute with reference to social media.	BTL1	Remembering
11	What is Freedom of Speech in online platforms?	BTL1	Remembering
12	Define Compliance Requirements in cybersecurity.	BTL1	Remembering
13	What is meant by data privacy?	BTL1	Remembering
14	Differentiate data privacy and data security.	BTL2	Understanding
15	What is a digital footprint?	BTL1	Remembering
16	List four user responsibilities.	BTL1	Remembering
17	What is plagiarism?	BTL1	Remembering
18	Define cyber ethics.	BTL1	Remembering
19	Name four international regulations.	BTL1	Remembering
20	Purpose of compliance requirements.	BTL2	Understanding
21	What is online defamation?	BTL1	Remembering
22	List four best practices for legal compliance.	BTL1	Remembering
23	Define Copyright and Patent.	BTL1	Remembering
24	List the different types of Intellectual Property Rights.	BTL1	Remembering

PART-B

Q.No.	Questions	Marks	BT Level	Competence
1	Analyze the role of international cyber laws in governing cyberspace and discuss the challenges involved in enforcing these laws across different countries.	(16)	BTL4	Analyzing
2	Evaluate the effectiveness of intellectual property laws in protecting digital content and software products.	(16)	BTL5	Evaluating
3	Analyze the impact of cyber piracy and copyright infringement on intellectual property protection.	(16)	BTL4	Analyzing
4	Evaluate the effectiveness of existing international cyber laws and treaties in addressing modern cyber threats.	(16)	BTL5	Evaluating
5	Apply the concept of Intellectual Property Rights (IPR) and discuss various forms such as copyrights, patents, trademarks, and trade secrets in the digital environment.	(16)	BTL3	Applying

6	Describe the significance of privacy policies in online platforms and explain their role in protecting user information.	(16)	BTL3	Applying
7	Analyze the major components of privacy policies and their implications for users and organizations.	(16)	BTL4	Analyzing
8	Describe the principles of ethical data use and discuss their importance in data collection, processing, and sharing.	(16)	BTL3	Applying
9	Evaluate the effectiveness of privacy policies in ensuring transparency and user trust in digital services.	(16)	BTL5	Evaluating
10	Analyze ethical issues related to big data analytics, artificial intelligence, and personal data usage.	(16)	BTL4	Analyzing
11	Develop guidelines for ethical data usage in organizations handling sensitive customer information.	(16)	BTL6	Creating
12	Analyze the responsibilities of users in maintaining cyber security and protecting digital assets.	(16)	BTL4	Analyzing
13	Analyze the role of user awareness and responsible online behavior in reducing cyber risks.	(16)	BTL4	Analyzing
14	Design a user awareness program to educate individuals about their cyber security responsibilities.	(16)	BTL6	Creating
15	Analyze the role of compliance requirements in ensuring information security and data protection.	(16)	BTL4	Analyzing
16	Analyze major legal disputes involving data privacy, copyright infringement, and cybercrime.	(16)	BTL4	Analyzing
17	Design a comprehensive cyber governance framework integrating international laws, privacy policies, ethical data use, and compliance requirements.	(16)	BTL6	Creating

UNIT V - ONLINE REPUTATION AND POLICIES				
Reputation Strategies-Brand Impact-Crisis Management-Corporate Communication -Social Media Policies-Governance Role-Monitoring Tools- Employee Training -Cybersecurity Integration.				
PART-A				
Q.No.	Questions	BT Level	Competence	
1	What is Online Reputation Management (ORM)?	BTL-1	Remember	
2	State the meaning of online reputation.	BTL-1	Remember	
3	Explain the importance of maintaining a positive online reputation.	BTL-2	Understand	
4	List the major reputation management strategies.	BTL-1	Remember	
5	Describe the impact of online reviews on brand image.	BTL-2	Understand	
6	Mention the objectives of reputation management.	BTL-1	Remember	
7	Recall the stages of crisis management.	BTL-1	Remember	
8	Discuss the purpose of corporate communication during a crisis.	BTL-2	Understand	
9	Name the components of a social media policy.	BTL-1	Remember	

10	Explain the role of governance in social media management.	BTL-2	Understand	
11	Describe how monitoring tools support reputation management.	BTL-2	Understand	
12	Identify any four online reputation monitoring tools.	BTL-1	Remember	
13	Define cybersecurity integration.	BTL-1	Remember	
14	Differentiate proactive and reactive reputation management.	BTL-2	Understand	
15	Specify the functions of corporate communication.	BTL-1	Remember	
16	Interpret the need for employee training in online reputation management.	BTL-2	Understand	
17	List the common sources of online reputation risks.	BTL-1	Remember	
18	State the objectives of a social media policy.	BTL-1	Remember	
19	Explain the relationship between cybersecurity and online reputation.	BTL-2	Understand	
20	Mention the benefits of governance in reputation management.	BTL-1	Remember	
21	Compare traditional and social media communication.	BTL-2	Understand	
22	Identify the factors affecting online reputation.	BTL-1	Remember	
23	Recall the significance of employee awareness programmes.	BTL-1	Remember	
24	Classify the different types of online reputation risks.	BTL-2	Understand	
	PART-B			
Q.No.	Questions	Marks	BT Level	Competence
1	Explain the reputation management strategies adopted by organizations with suitable examples.	(16)	BTL-4	Analyze
2	Analyze the impact of online reputation on brand image and business growth.	(16)	BTL-4	Analyze
3	Develop a social media policy for an organization to protect its online reputation.	(16)	BTL-3	Apply
4	Evaluate the effectiveness of governance practices in online reputation management.	(16)	BTL-5	Evaluate
5	Illustrate the crisis management process for handling an online reputation crisis.	(16)	BTL-3	Apply
6	Examine the role of corporate communication in restoring organizational reputation.	(16)	BTL-4	Analyze
7	Assess the effectiveness of monitoring tools in protecting online reputation.	(16)	BTL-5	Evaluate
8	Apply suitable monitoring tools to identify and respond to online reputation threats.	(16)	BTL-3	Apply
9	Analyze the significance of employee training in minimizing reputation risks.	(16)	BTL-4	Analyze
10	Evaluate the contribution of cyber security integration to reputation management.	(16)	BTL-5	Evaluate

11	Demonstrate governance mechanisms for responsible social media usage.	(16)	BTL-3	Apply
12	Investigate the effectiveness of online reputation monitoring tools.	(16)	BTL-4	Analyze
13	Prepare a corporate communication plan for managing an online reputation crisis.	(16)	BTL-3	Apply
14	Evaluate the effectiveness of an organization's social media policy in preventing reputational damage.	(16)	BTL-5	Evaluate
15	Analyze the relationship between corporate communication, governance, and reputation management.	(16)	BTL-4	Analyze
16	Illustrate cybersecurity integration with reputation management using suitable examples.	(16)	BTL-3	Apply
17	Assess the effectiveness of employee awareness programmes in protecting organizational reputation.	(16)	BTL-5	Evaluate

Faculty In-Charge

Verified by

HOD