Lesson Plan No. 2.1	Course Name: Cyber Security Foundations Topic: Classification of Cyber Crimes	Course No.: BBALLB-506

Objectives	At the end of the lesson the student shall be able to: a. Understand the classification of cyber crimes. b. Identify different categories of cyber crimes targeting computers and mobiles. c. Discuss examples of common cyber crimes.
Teaching Aids (if any)	a. Presentation
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What comes to mind when you hear "cyber crime"? - Why do you think cyber crimes target computers and mobile devices? 2. Introduction - Brief overview of cyber crime classification. **Development** (30 minutes) 3. Explain categories of cyber crimes: targeting systems, targeting individuals, targeting governments. 4. Discuss examples of crimes targeting computers and mobiles: phishing, identity theft, unauthorized access. **Exercise** (5 minutes): 5. Identify types of crimes in given scenarios.
Closure	1. Summarize key points. 2. Reflective questions about classifications. 3. Suggested Reading: - Textbook 1, Chapter 2, pp. 45-65. Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the different classifications of cyber crimes? - How do cyber crimes differ in targeting systems vs. individuals? 2. Homework: - Research and write a brief report on a recent case involving cyber crime targeting mobiles. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.2	Course Name: Cyber Security Foundations Topic: Cyber Crime Against Women and Children	Course No.: BBALLB-506

Objectives	At the end of the lesson the student shall be able to: a. Understand the unique nature of cyber crimes against women and children. b. Identify examples of crimes specific to these groups. c. Discuss legal protections and reporting mechanisms.
Teaching Aids (if any)	a. Presentation
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - Why do you think cyber crimes against women and children are on the rise? - What protections should be in place to guard against these crimes? 2. Introduction - Brief overview of cyber crimes against vulnerable groups. **Development** (30 minutes) 1. Explain specific cyber crimes: harassment, cyberstalking, exploitation. 2. Discuss protections in place and the importance of reporting. **Exercise** (5 minutes): 3. Analyze a case study of a cyber crime affecting women or children. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 3, pp. 66-85. Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the specific crimes targeting women and children? - How does the law protect these vulnerable groups? 2. Homework: - Write a summary of a recent case involving cyber crime against women or children. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.3	Course Name: Cyber Security Foundations Topic: Financial Frauds and Social Engineering Attacks	Course No.: BBALLB-506

Objectives	At the end of the lesson the student shall be able to: a. Understand the concept of financial frauds in cyberspace. b. Identify common social engineering techniques. c. Discuss ways to recognize and prevent these attacks.
Teaching Aids (if any)	a. Presentation
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you think constitutes financial fraud online? - How can someone manipulate information to deceive others? 2. Introduction - Brief overview of financial frauds and social engineering. **Development** (30 minutes) 1. Explain social engineering tactics: phishing, pretexting, baiting. 2. Discuss the importance of user awareness and education. **Exercise** (5 minutes): 3. Identify red flags in simulated phishing emails. Use Nearpod to collect responses and discuss the answers.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 4, pp. 86-110. Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - How can individuals recognize social engineering tactics? - What steps can users take to protect themselves? 2. Homework: - Research and report on a financial fraud case involving social engineering. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.4	Course Name: Cyber Security Foundations Topic: Malware and Ransomware Attacks	Course No.: BBALLB-506

Objectives	At the end of the lesson the student shall be able to: a. Understand malware and ransomware threats. b. Identify how malware and ransomware infect systems. c. Discuss methods for prevention and protection..
Teaching Aids (if any)	a. Presentation
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - Have you heard of ransomware attacks in the news? - What security practices can prevent malware infection? 2. Introduction - Brief overview of malware and ransomware. **Development** (30 minutes) 1. Explain types of malware: viruses, worms, ransomware. 2. Discuss strategies for prevention: antivirus, backups, security patches. **Exercise** (5 minutes): 3. Analyze ransomware threats and discuss preventive measures.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 5, pp. 111-135. Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are common malware types? - How can users prevent ransomware infection? - Evaluation Tool: Quiz on malware and ransomware attacks. 2. Nearpod Quiz on User-Side Web Security 3. Homework: - Write a summary of a recent ransomware attack and how it was resolved. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.5	Course Name: Cyber Security Foundations Topic: Zero-Day and Zero-Click Attacks	Course No.: BBALLB-506

Objectives	At the end of the lesson the student shall be able to: a. Understand the concept of zero-day and zero-click vulnerabilities. b. Identify the impact of these attacks on system security. c. Discuss methods to mitigate zero-day threats.
Teaching Aids (if any)	a. Presentation
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you know about zero-day vulnerabilities? - Why might they be challenging to detect and prevent? 2. Introduction - Brief overview of zero-day and zero-click attacks. **Development** (30 minutes) 1. Explain zero-day exploits and how they are used in attacks. 2. Discuss zero-click attacks and their unique challenges. **Exercise** (5 minutes): 3. Review case studies of zero-day attacks.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 5, pp. 136-150. Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are zero-day and zero-click vulnerabilities? - How can organizations protect against zero-day attacks? 2. Homework: - Write a report on a recent zero-day attack and the response to it. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.6	Course Name: Cyber Security Foundations Topic: Modus Operandi of Cybercriminals	Course No.: BBALLB-506

Objectives	At the end of the lesson the student shall be able to: a. Understand the modus operandi of cybercriminals. b. Identify techniques used by cybercriminals to exploit victims. c. Discuss how users can protect themselves against these tactics.
Teaching Aids (if any)	a. Presentation
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What tactics do cybercriminals use to deceive victims? - How can one recognize these tactics? 2. Introduction - Brief overview of cybercriminals' methods. **Development** (30 minutes) 1. Discuss tactics like phishing, social engineering, malware injection. 2. Explain red flags and self-protection methods. **Exercise** (5 minutes): 3. Analyze case scenarios demonstrating cybercriminal techniques.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 6, pp. 151-170 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - How do cybercriminals exploit victims? - What are key strategies for recognizing criminal tactics? 2. Homework: - Write a summary of a recent attack involving cybercriminal tactics. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.7	Course Name: Cyber Security Foundations Topic: Reporting of Cyber Crimes	Course No.: BBALLB-506

Objectives	At the end of the lesson the student shall be able to: a. Understand the different types of web attacks targeting users. b. Learn how these attacks compromise user data. c. Discuss the methods used to execute these attacks. d. Evaluate strategies to protect against web attacks targeting users.
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you do to protect your personal information online? - Have you ever been a victim of a web attack? 2. Introduction - Overview of web attacks targeting users. **Development** (30 minutes) 3. Explain types of web attacks: phishing, social engineering, clickjacking. 4. Discuss how these attacks compromise user data. 5. Show video to explain web attacks. **Exercise** (5 minutes): 6. Analyze case scenarios demonstrating cybercriminal techniques.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 6, pp. 151-170. Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - How do cybercriminals exploit victims? - What are key strategies for recognizing criminal tactics? 2. Homework: - Write a summary of a recent attack involving cybercriminal tactics. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.7	Course Name: Cyber Security Foundations Topic: Reporting of Cyber Crimes	Course No.: BBALLB-506

Objectives	At the end of the lesson the student shall be able to: a. Understand the importance of reporting cyber crimes. b. Identify reporting mechanisms available to victims. c. Discuss the role of law enforcement in cybercrime investigation.
Teaching Aids (if any)	a. Presentation
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - Why do you think reporting cyber crimes is important? - How can law enforcement help victims of cyber crime? 2. Introduction - Brief overview of cyber crime reporting. **Development** (30 minutes) 1. Explain reporting methods: local authorities, CERT-IN, online portals. 2. Discuss the role of law. **Exercise** (5 minutes): 3. Analyze a recent data breach incident.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 6, pp. 171-185 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the current options for us to report cyber crimes? - Which organizations are working to curb cybercrimes in our country? 2. Homework: - Research a major data breach and prepare a report on its impact. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.8	Course Name: Cyber Security Foundations Topic: Remedial and Mitigation Measures	Course No.: BBALLB-506

Objectives	At the end of the lesson the student shall be able to: a. Understand common remedial and mitigation measures for cyber threats. b. Identify strategies for minimizing the impact of cyber attacks. c. Discuss tools and techniques to remediate compromised systems.
Teaching Aids (if any)	a. Presentation
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What actions would you take if you discovered a security breach? - Why is it important to have a response plan for cyber attacks? 2. Introduction - Brief overview of remediation and mitigation strategies. **Development** (30 minutes) 1. Explain strategies like backups, patches, and updates. 2. Discuss techniques for incident containment, eradication, and recovery. **Exercise** (5 minutes): 3. Analyze a case study on mitigation measures taken after an attack.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 7, pp. 186-200. Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are common measures to mitigate cyber threats? - How can organizations recover from a cyber attack? 2. Homework: - Research a recent cyber attack and report on the mitigation measures used. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.9	Course Name: Cyber Security Foundations Topic: Legal Perspective of Cyber Crime	Course No.: BBALLB-506

Objectives	At the end of the lesson the student shall be able to: a. Understand the legal framework surrounding cyber crime. b. Identify key provisions of the IT Act 2000 and its amendments. c. Discuss how laws protect against cyber crimes and hold offenders accountable
Teaching Aids (if any)	a. Presentation b. Chalkboard/Whiteboard c. Use of Nearpod tool for online quiz
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What do you think are the legal consequences of cyber crime? - Why is it essential to have laws specifically addressing cyber crime? 2. Introduction - Brief overview of the legal perspective of cyber crime. **Development** (30 minutes) 1. Explain key provisions of the IT Act 2000 and its amendments. 2. Discuss notable cases and legal consequences. **Exercise** (5 minutes): 3. Analyze a case study on a legal proceeding related to cyber crime.
Closure	1. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 2. Suggested Reading - Textbook 1, Chapter 8, pp. 201-215 Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	1. Reflective Questions - What are the key provisions of the IT Act? - How do laws protect against cyber crime? 2. Homework: - Write a report on a notable cyber crime case and the legal outcome. Spend 5 minutes to evaluate student assimilation of the lesson contents

Lesson Plan No. 2.10	Course Name: Cyber Security Foundations Topic: Ethical Issues in Cyber Security and Incident Analysis	Course No.: BBALLB-506

Objectives	At the end of the lesson the student shall be able to: a. Understand ethical issues related to cyber security. b. Identify the importance of ethics in incident analysis. c. Discuss ethical considerations in handling cyber crime and security incidents
Teaching Aids (if any)	a. Presentation
Teaching Development	**Introduction** (5 minutes) 1. Pre-discussion Questions - What ethical dilemmas might arise in cyber security? - Why is it essential to handle cyber crime cases with ethical consideration? 2. Introduction - Brief overview of ethics in cyber security. **Development** (30 minutes) 3. Explain common ethical issues: privacy vs. security, data sharing, responsible disclosure. 4. Discuss the role of ethics in incident response and analysis. **Exercise** (5 minutes): 5. Evaluate ethical dilemmas in simulated scenarios related to cyber incidents.
Closure	3. Summarize the Lesson Learning Outcomes and get affirmation from students on these. 4. Suggested Reading - Textbook 1, Chapter 8, pp. 216-230. Spend 5 minutes to wrap up and consolidate the learnings
Evaluation	3. Reflective Questions - What are common ethical issues in cyber security? - How can ethical considerations shape incident analysis? 4. Homework: - Write a reflection on an ethical issue in a recent cyber crime case. Spend 5 minutes to evaluate student assimilation of the lesson contents