COURSE HANDOUT

CYBER SECURITY FOUNDATIONS - BBALLB-5010 (A)

BBALLB – 5th SEMESTER

ACADEMIC YEAR (2024-25)

Mr. Azra Ashraf Shah

Assistant Professor

Department of Computer Science and Engineering

Department of Computer Science and Engineering

Model Institute of Engineering & Technology (Autonomous)

Kot Bhalwal, Jammu - 181122

www.mietjmu.in

Course Code	Course Name	Course Type	Cd	L	T	P	Marks		
							Sessional	Final Exam	Total
BBALLB-5010 (A)	Cyber Security Foundations	Elective	4	4	0	0	30	70	100

COURSE OUTCOMES

At the end of the course the student will be able to:	
CO1	Describe the architecture of cyberspace, internet governance, and the challenges of cyber security.
CO2	Analyze various types of cybercrimes, their impact, and the legal frameworks addressing them.
CO3	Evaluate security issues and best practices related to the use of social media platforms.
CO4	Examine the security aspects of e-commerce and digital payments, including legal guidelines and preventive measures.
CO5	Implement security best practices and tools to protect digital devices and manage cyber threats.

Unit-I: Introduction to Cyber Security

1.1 Defining Cyberspace and Overview of Computer and Web-technology
1.2 Architecture of Cyberspace, Communication and Web Technology, Internet, World Wide Web
1.3 Advent of Internet, Internet Infrastructure for Data Transfer and Governance
1.4 Internet Society and Regulation of Cyberspace
1.5 Concept of Cyber Security, Issues and Challenges of Cyber Security.

(08 Hours)

Unit-II: Cyber Crime and Cyber Law

2.1 Classification of Cyber Crimes, Common Cyber Crimes - Cyber Crime Targeting Computers and Mobiles
2.2 Cyber Crime against Women and Children, Financial Frauds, Social Engineering Attacks, Malware and Ransomware Attacks, Zero Day and Zero Click Attacks
2.3 Cybercriminals Modus-operandi, Reporting of Cyber Crimes
2.4 Remedial and Mitigation Measures
2.5 Legal Perspective of Cyber Crime, IT Act 2000 and Its Amendments, Cyber Crime and Offences

(10 Hours)

Unit-III: Social Media Overview and Security

3.1 Introduction to Social Networks
3.2 Types of Social Media, Social Media Platforms,
3.3 Social media monitoring, Hashtag, Viral Content, Social Media Marketing
3.4 Social Media Privacy, Challenges, Opportunities and Pitfalls in Online Social Network, Security Issues related to Social Media, Flagging and Reporting of Inappropriate Content
3.5 Best practices for the use of Social Media

(08 Hours)

Unit-lV: E-Commerce and Digital Payments

4.1 Definition of E-Commerce, Main Components of E-Commerce, Elements of E-Commerce Security, E-Commerce
Threats, E-Commerce Security Best Practices
4.2 Introduction to Digital Payments, Components of Digital Payment and Stake Holders
4.3 Modes of Digital Payments – Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhar Enabled Payments, Digital Payments related Common Frauds and Preventive Measures
4.4 RBI Guidelines on Digital Payments and Customer Protection in Unauthorised Banking Transactions
4.5 Relevant Provisions of Payment Settlement Act, 2007

(12 Hours)

Unit-V: Digital Devices Security, Tools and Technologies for Cyber Security

5.1 End Point Device and Mobile Phone Security, Password Policy, Security Patch Management, Data Backup

5.2 Downloading and Management of Third Party Software
5.3 Device Security Policy, Cyber Security Best Practices
5.4 Significance of Host Firewall and Ant-virus, Management of Host Firewall and Anti-virus, Wi-Fi Security
5.5 Configuration of Basic Security Policy and Permissions.

(10 Hours)

Hands-On Practice Sessions:	
1.	Checklist for reporting cyber crime at cyber crime Police Station.
2.	Checklist for reporting cyber crime online
3.	Reporting phishing emails
4.	Demonstration of email phishing attack and preventive measures
5.	Basic checklist, privacy and security settings for popular social media platforms
6.	Reporting and redressal mechanism for violations and misuse of Social media platforms.
7.	Configuring security settings in Mobile Wallets and UPIs.
8.	Checklist for secure net banking
9.	Setting, configuring and managing three password policy in the computer (BIOS, Administrator and Standard User)
10.	Setting and configuring two factor authentication in the Mobile phone
11.	Security patch management and updates in Computer and Mobiles
12	Managing Application permissions in Mobile phone
13.	Installation and configuration of computer Anti-virus.
14.	Installation and configuration of Computer Host Firewall
15.	Wi-Fi security management in computer and mobile.

Textbooks

S. No.	Name of the Books	Name of the Author	Publisher Name	Edition (Pub. Yr.)
1	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives	Nina Godbole & Sunit Belapure	**Wiley**	**2011**
2.	Fundamental of Cyber Security (Principles, Theory and Practices)	Mayank Bhushan, Rajkumar Singh Rathore, Jamshed Aatif	BPB Publisher	2020

Reference Books

S. No.	Name of the Books	Name of the Author	Publisher Name	Edition (Pub. Yr.)
1	Cybersecurity Fundamentals	Rajesh Kumar Goutam	BPB Publisher	2021
2	Cyber Crime Impact in the New Millennium	R. C Mishra	Auther Press	2010

COURSE PLAN		
Unit-I Introduction to Cyber Security		
S. No	**Topics**	**Recommended Books**
1	Defining Cyberspace and Overview of Computer and Web-technology	Book 1, Ch.1
2	Architecture of Cyberspace, Communication and Web Technology, Internet, World Wide Web	Book 1, Ch.1
3	Advent of Internet, Internet Infrastructure for Data Transfer and Governance	Book 1, Ch.1
4	Internet Society and Regulation of Cyberspace	Book 2, Ch.2
5	Concept of Cyber Security, Issues and Challenges of Cyber Security	Book 2, Ch.2
Unit-II Cyber Crime and Cyber Law		
6	Classification of Cyber Crimes,	Book 1, Ch.2
7	Cyber Crime against Women and Children,	Book 1, Ch.2
8	Cybercriminals Modus-operandi,	Book 1, Ch.1
9	Remedial and Mitigation Measures	Book 2, Ch.2
10	Legal Perspective of Cyber Crime, IT Act 2000 and Its Amendments, Cyber Crime and Offences	Book 2, Ch.2
11	Financial Frauds, Social Engineering Attacks, Malware and Ransomware Attacks, Zero Day and Zero Click Attacks	Book 2, Ch.2
12	Reporting of Cyber Crimes	Book 2, Ch.2
15	Common Cyber Crimes - Cyber Crime Targeting Computers and Mobiles	Book 2, Ch.2
Unit-III Social Media Overview and Security		
16	Introduction to Social Networks	Book 2, Ch.2
17	Types of Social Media, Social Media Platforms,	Book 2, Ch.2
18	Social media monitoring, Hashtag, Viral Content, Social Media Marketing	Book 2, Ch.2
19	Social Media Privacy, Challenges, Opportunities and Pitfalls in Online Social Network,	Book 2, Ch.2
20	Best practices for the use of Social Media	Book 2, Ch.2
21	Security Issues related to Social Media, Flagging and Reporting of Inappropriate Content	Book 2, Ch.2
Unit-IV E-Commerce and Digital Payments		
22	Definition of E-Commerce, Main Components of E-Commerce, Elements of E-Commerce Security, E-Commerce	Book 2, Ch.3
23	Threats, E-Commerce Security Best Practices	Book 1, Ch.4
24	4.2 Introduction to Digital Payments, Components of Digital Payment and Stake Holders	Book 1, Ch.4
25	4.3 Modes of Digital Payments – Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured	Book 2, Ch.3
26	Supplementary Service Data (USSD), Aadhar Enabled Payments, Digital Payments related Common Frauds and	Book 1, Ch.3
27	Preventive Measures	Book 2, Ch.3

28	4.4 RBI Guidelines on Digital Payments and Customer Protection in Unauthorised Banking Transactions	Book 1, Ch.3
Unit-V Digital Devices Security, Tools and Technologies for Cyber Security		
29	End Point Device and Mobile Phone Security, Password Policy, Security Patch Management, Data Backup	Book 2, Ch.8
30	Downloading and Management of Third Party Software	Book 1, Ch.8
31	Device Security Policy, Cyber Security Best Practices	Book 2, Ch.8
32	Significance of Host Firewall and Ant-virus, Management of Host Firewall and Anti-virus, Wi-Fi Security	Book 1, Ch.8
33	Configuration of Basic Security Policy and Permissions.	Book 2, Ch.8
34	End Point Device and Mobile Phone Security, Password Policy, Security Patch Management, Data Backup	Book2, Ch. 8
35	Downloading and Management of Third Party Software	

ADDITIONAL WEB RESOURCES

1.	**MOOCs:** 1. Introduction to Computers and Operating Systems and Security | Microsoft 2. Cybersecurity Threat Vectors and Mitigation | Microsoft 3. Cybersecurity Identity and Access Solutions using Azure AD | Microsoft 4. Foundations of Cybersecurity | Google
2.	**YouTube:** Cyber Security Full Course | Simplilearn

GRADING AND ASSESSMENT

- **Sessional Test**: 10 marks
- **Assignment**: 10 marks
- **Attendance**: 10 marks
- **Final Examination**: 70 marks

COURSE POLICIES

- **Attendance**: Minimum 75% attendance is mandatory to appear in the final examination of the course.
- **Academic Integrity**: MIET's academic integrity policies apply. Plagiarism will not be tolerated.
- **Late Submissions**: Assignments and projects must be submitted by the specified timelines.

FACULTY INFORMATION

- **Office Hours**

  Mon- 1:00PM to 1:30 PM
- **Contact Information**
  azra..cse@mietjammu.in |