Dt: 09.12.2024

To,
The Registrar,
Mahatma Gandhi University,
Nalgonda,

Sir,

Sub: Submission of Revised syllabus for cyber Security Course (GE) for all UG & BBA programmes- Reg.

The University vide order Lr.no. 182/MGU/AAC/NLG/2024-25, dated 25.11.2024, a committee was constituted for the revision of syllabus for cyber Security Course (GE) for all UG & BBA programmes.

The committee members met on 4th, 6th and 9th December at Department of Computer Science and informatics, UCET, MGU. After through discussion in three meetings the committee has recommended for revise the syllabus for cyber Security Course (GE) for all UG & BBA programmes. Revised syllabus is enclosed along with this letter.

Committee members present are:

1. Prof. R. Rekha	Chairperson	Rekha 9/12/2024
2. Ms. Ch. Sudha Rani	Member	CH. Sudha
3. Dr. D. Sandhya Rani	Member	Rani 9/12/2024
4. Dr. K. Harish Kumar	Member	09/12/2024
5. Dr. M. Jayanthi	Convener	Jayanthi 09/12/24

Dean, CDC
fr nlg
11/12

Revised Syllabus of Cyber Security Course / Program at Undergraduate Level

[Total 45 Teaching Hours=3 Credits, 30 Practical Hours =1 Credit,
Total No. of Credits=4]

Module -I Introduction to Cyber Security

Definition of Cyber Security and Web-technology: Definition and basics of Computers, Electronic Devices, Operating Systems, Cyber Safety, Cyber Security, CIA Triad (Confidentiality, Integrity & Availability of Information), Fundamentals of Digital Hygiene, Types of Cyber Threats. Architecture of Cyberspace, Communication and Web technology, Internet, World Wide Web, Advent of Internet, Internet infrastructure for data transfer and governance, Internet society.

Regulation of Cyberspace: Cyber Security Mechanisms, need and modes of Cryptography, Encryption, Firewalls, Passwords, Privacy, Digital Signatures-Issues and challenges of cyber security.

Emerging Technologies & Trends: IPv4(Internet Protocol Version)v/s IPv6, IOT(Internet of Things), Machine Learning, Artificial Intelligence, Crypto currency and Block Chain Technology, Cloud Computing, Web 3, and Dark Web.

The outcome of learning: After completing this module, students will understand the concept of cyberspace, cyber security and its associated issues and challenges. They would understand the main components of a cyber security plan. They would also get basic insights into risk-based assessment and the requirement of security controls.

Module –II: Introduction to Cyber Laws and Cyber Crime

Introduction to Cyber Law: An overview of Information Technology Act 2000. Definition of basic legal terms of IT law, Investigative framework, the role of *Cert-In* in Collection, Dissemination, and Advisories on cyber-crimes incidence, Legal recognition of Electronic Records and Electronic Signatures, Functions and liabilities of IT Intermediaries, Basics of SPDI (Sensitive Personal Data or Information) Rules 2011

Definition of Cyber-Crimes under IT Act 2000.

Types of Cyber Crimes: Hacking (Computer Viruses, Time Bombs, Trojans, Malicious Code "Malware", DOS, DDOS, Web defacement, Phishing, cloning, financial frauds, social engineering attacks, malware and ransom ware attacks, zero-day and zero click attacks), Cyber Stalking, Cyber Bullying, Cyber Pornography, Child Pornography, Cyber Laundering, Online betting and games, Violation of Cyber Privacy, Voyeurism, Data Privacy, Data Theft, and Cyber Terrorism.

Cyber Crime Investigation: Cyber Crime Cells, Reporting of Cyber Crimes, Cyber Investigation

The outcome of learning: Students, by the end of this module should be able to understand the basics of IT law in India, legal remedies and how to report crimes through available platforms. They are also expected to learn about government initiatives to curb cyber-crimes and IT intermediaries' functions and liabilities. They are also able to understand the concept of Cybercrimes, their nature, legal remedies, protection and punishments.

Module-III: Basics of Electronic Governance and Social Network

Electronic Governance: Definition, Distinction between E-Government, Internet Governance and e-Governance.

Cyber Ethics & Responsible Digital Citizenship: Understanding ethical considerations in digital realm, Importance and responsibility of maintaining data integrity, Importance of respect for others' privacy and security, Respecting Intellectual Property Rights & avoiding plagiarism, Promoting online inclusivity, diversity and digital etiquette, Consequences of unethical and illegal practices, Individual Social Responsibility of spreading awareness on Digital privacy, safety & security.

Social Media & Internet Messaging Safety: Architecture of Social Media Platforms, Types of Social Media Platforms, Trends in Social Media Platforms (including Deep Fakes, Sock puppets), Procedure of Collaborating Securely and ethically on Social Media Platform, Privacy v/s Social Media Platform, Free Speech v/s Mis/Mal/Dis Information, Vulnerable and secure practices on Social Media - Sharing of personal information like Personal Identifiable Information(PII) details, locations, photographs, etc. Managing Social Media Privacy & Security settings, Cyber Bullying & its consequences, Internet Messaging Platforms, Effective Communication Skills on Digital Platforms.

The outcome of learning: Students, after completion of this module, would understand the concept of e-governance and Social Network.

Module IV: Social Network Security

Social Media Monitoring and Privacy: Hashtags, viral content, social media marketing, privacy violation challenges and pitfalls in the online social network. Flagging and reporting of inappropriate content, Rules and regulations regarding posting of inappropriate content, Issues involving Cyber security for social media, Privacy of Data, Data Mining, Virus and Malware Attacks.

Social Engineering Awareness: Definition of Social Engineering techniques & tactics in Cyber Frauds, Methods of identifying and preventing social engineering cybercrimes like Impersonation, Mule Identity, Identity Theft, Phishing, Spear Phishing, Pretexting, Baiting, Scareware, Tailgating, Quid Pro Quo, etc

Issues concerning the use of 3rd Party Applications: Legal Issues, Risks & Challenges, Identity Theft, Romance Scams, Whistle-blowers, Cyber Stalking, Cyber Bullying, Cyber Terrorism, Best practices for the use of social media and ensuring cyber security.

Introduction to OSINT Framework (Open-Source Intelligence tools)

The outcome of learning: In this module, students would be able to conduct online investigative research and data collection using Open Source Intelligence Tools (OSINT), identify risks to users from OSINT data collection and explain countermeasures to be utilized in providing anonymity for users. enhance and customize the art of using OSINT techniques for collecting information for intelligence and counterintelligence purposes.

Module V: E-Commerce and Cyber Security

Basics of E-Commerce: Concept and meaning, Different models of e-commerce.

Banking & Financial Services Safety: Understanding digital banking and financial services, Various types of digital banking and financial services, Secure Banking Practices, Importance of authentication and passwords, Importance of software updation and security patches, Vulnerabilities and consequences of Digital Loan System.

Introduction to digital payments: Components of digital payment and stakeholders, **Modes of digital payments:** Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhar enabled payments, Digital payments related to common frauds and preventive measures.

E-Commerce threats: E-Commerce security and its best practices.

Elements of E-Commerce security: Secure Socket Layering (SSL), Hyper Text Transfer Protocol (HTTP), Hyper Text Transfer Protocol Security (HTTPS), and Password encryption.

E-Commerce Rules under Consumer Protection Act 2019

The outcome of learning: After completing this module, students would be able to understand the basic concepts related to E-Commerce and digital payments threats, various digital payment modes and related cyber security aspects.

Practical Exercises

1. Authentication Management: Definition and importance of authentication, types of authentications – Facial, Iris, Finger print, Palm print, multi-factor, Use of authentication – places where authentication access should be used.
2. Password Management: Importance of password management, creation of strong, unique & secure password, techniques of maintaining passwords over various platforms, updating of passwords regularly, password management tools and practices.
3. Secure Internet Browsing: Understanding secure connections (HTTPS) & avoiding untrusted networks, Web browser security settings & extensions.
4. List out security controls for the computer and implement technical security controls in the personal computer. List out security controls for mobile phones and implement technical security controls in the personal mobile phone. Installation and configuration of anti-virus software, computer host firewall. Wi-Fi security management in desktop machines and mobile devices.

Ch. Sudha

5. Visit police stations.
6. Visit E-Seva Centers/e-Governance portals for understanding various e-Governance schemes and their legal frameworks.
7. Visiting public authorities receiving / disposing RTI applications online.
8. Demonstration of DDOS, DNS Poisoning attacks, SQL Attacks, Malware and Ransomware attacks and creating awareness on preventive measures.
9. Expertise in effectively responding to a Cybercrime incident.
10. Checklist for reporting cybercrimes on NCRP (https://cybercrime.gov.in/)
11. Setting of privacy and security mechanism in social media networks
12. Use social media intelligence paradigms on social media handles like Facebook, Twitter, Instagram, LinkedIn, etc.
13. Review, monitor and evaluate search engine information from the dark web from Google, Bing, Yahoo, and others.
14. Monitoring information on Websites, Directories, search engines, and meta-search engines, as well as reviewing user activity on digital platforms for gathering information on the entities involved in the crime scenes.
15. Access old cached data from the internet using Website analysis and data collection.
16. Identify fake profiles, sock puppets, fake emails, and mail addresses from social networks or Google results.
17. Configuring security settings in Mobile Wallets and UPI.
18. Case Studies related to E-Commerce and various digital payments modes and related cyber security aspects.

Note: The visits may be physical or virtual. Further the above public authorities institutions are illustrative in nature

References

1. Cyber Crime Impact in the New Millennium, R. C Mishra, Auther Press. Edition 2010.
2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives Sumit Belapure and Nina Godbole, Wiley India Pvt.

Ltd. (First Edition, 2011)

3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
4. Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
5. Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
6. Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.
7. Fundamentals of Network Security E. Maiwald, McGraw Hill.