Semester: VI	Internal Marks: 25		External Marks: 75	
COURSE CODE	**COURSE TITLE**	**CATEGORY**	**HOURS/WEEK**	**CREDITS**
22UGCS	**CYBER SECURITY**	**CC**	**3(T) + 2(P)**	**4**

Course Objective

- To understand the concept of Cyber security and the issues and challenges associated with it
- To develop an understanding of cyber crimes, their nature, and legal remedies
- To appreciate various privacy and security concerns on online Social media
- To analyze and evaluate the basic concepts related to E-Commerce and digital payments
- To analyze and evaluate the basic security aspects related to Computer and Mobiles

Course Outcome and Cognitive Level Mapping

On the successful completion of the course, students will be able to

CO Number	CO Statement	Cognitive Level
CO1	Outline the concept of cyber security, cyber crime, cyber law and the issues and challenges	K1
CO2	Deeper understanding and familiarity with cyber crimes, their nature, and legal remedies using case studies	K2
CO3	Apply various privacy and security concerns on Social media & online payments	K3
CO4	Analyze the tools & techniques for cyber security	K4
CO5	Evaluate the security aspects of Computer, Mobiles & Other digital devices	K5

Mapping of CO with PO and PSO

COs	PSO1	PSO2	PSO3	PSO4	PSO5	PO1	PO2	PO3	PO4	PO5
CO1	3	1	3	3	3	3	1	2	3	3
CO2	3	2	3	3	3	3	2	2	3	3
CO3	3	2	3	3	3	3	2	3	3	3
CO4	3	2	3	3	3	3	2	3	3	3
CO5	3	2	3	3	3	3	2	3	3	3

"1"- Slight (Low) Correlation
"2"– Moderate (Medium) Correlation
"3"- Substantial (High) Correlation
"-"- Indicates there is no Correlation

Syllabus

Theory

UNIT	CONTENT	HOURS	COs	COGNITIVE LEVEL
I	**Introduction to Cyber Security:** Defining Cyberspace and Overview of Computer and Web-technology, 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, Concept of cyber security, Issues and challenges of cyber security.	9	CO1 CO2 CO3	K1 K2 K3
II	**Cyber Crime and Cyber Law:** Classification of cyber crimes, Common cyber crimes- cyber crime targeting computers and mobiles, cyber crime against women and children, financial frauds, social engineering attacks, malware and ransomware attacks, zero day and zero click attacks, Cybercriminals modus-operandi , Reporting of cyber crimes, Remedial and mitigation measures, Legal perspective of cyber crime, IT Act 2000 and its amendments, Cyber crime and offences, Organisations dealing with Cyber crime and Cyber security in India.	9	CO1 CO2 CO3 CO4	K1 K2 K3 K4
III	**Social Media Overview and Security:** Introduction to Social networks. Types of Social media, Social media platforms, Social media monitoring, Hashtag, Viral content, Social media marketing, Social media privacy, Challenges, opportunities and pitfalls in online social network, Security issues related to social media, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content, Best practices for the use of Social media.	9	CO1 CO2 CO3 CO4	K1 K2 K3 K4
IV	**E-Commerce and Digital Payments:** Definition of E- Commerce, Main components of E-Commerce, Elements of E-Commerce security, E-Commerce threats, E-Commerce security best practices, Introduction to digital payments, Components of digital payment and stake holders, Modes of digital payments- Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhar	9	CO1 CO2 CO3 CO4 CO5	K1 K2 K3 K4 K5

	enabled payments, Digital payments related common frauds and preventive measures. RBI guidelines on digital payments and customer protection in unauthorized banking transactions. Relevant provisions of Payment Settlement Act, 2007.			
V	**Digital Devices Security , Tools and Technologies for Cyber Security:** End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third party software, Device security policy, Cyber Security best practices, Significance of host firewall and Anti-virus, Management of host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions.	9	CO1 CO2 CO3 CO4 CO5	K1 K2 K3 K4 K5
VI	**Self Study for Enrichment** **(Not included for End Semester Examinations)** **Case Studies:** Parliament Attack Cyber Crime - Pune Citibank MphasiS Call Center Fraud, Yahoo Data Breach, Equifax Data Breach	-	CO2 CO3 CO4 CO5	K2 K3 K4 K5

Reference Books

1. R. C Mishra, (2010) *Cyber Crime: Impact on the New Millennium*, Authors Press. Edition 2010.
2. Sunit Belapure and Nina Godbole, (2011). *Cyber Security Understanding Cyber Crimes*, Computer Forensics and Legal Perspectives, Wiley India Pvt. Ltd., First Edition.
3. Henry A. Oliver, (2015) *Security in the Digital Age: Social Media Security Threats and Vulnerabilities*, Create Space Independent Publishing Platform, Pearson.
4. Elias M. Awad, (2001) *Electronic Commerce*, Prentice Hall of India Pvt Ltd.
5. Krishna Kumar, (2011) *Cyber Laws: Intellectual Property & E-Commerce Security*, Dominant Publishers.
6. Eric Cole, Ronald Krutz, (2011) *Network Security Bible*, Wiley India Pvt. Ltd, 2nd Edition.
7. E. Maiwald , (2017) *Fundamentals of Network Security*, McGraw Hill.

Web References

1. https://www.udacity.com/course/intro-to-cybersecurity-nanodegree--nd545
2. https://www.vidhikarya.com/legal-blog/cyber-crime-and-cyber-law-in-india
3. https://www.techtarget.com/searchsecurity/definition/cybersecurity
4. https://www.financemagnates.com/fintech/payments/the-evolution-of-digital-payments-and-e-commerce/
5. https://www.javatpoint.com/cyber-security-tools
6. https://www.cyberralegalservices.com/casestudies.php
7. https://www.kroll.com/en/insights/publications/cyber/case-studies

Practical

List of Exercises: (Not included for End Semester Examinations)

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.

Web References

1. https://cybercrime.gov.in/
2. https://cybercrime.gov.in/webform/crime_onlinesafetytips.aspx
3. https://www.digitalvidya.com/blog/social-media-dos-and-donts/
4. https://www.medianama.com/2023/02/223-platform-grievance-appellate-committees-social-media/
5. https://www.ibm.com/topics/security-controls
6. https://docs.oracle.com/cd/E19683-01/817-0365/concept-2/index.html

Pedagogy

Chalk and Talk, Group discussion, Seminar & Assignment.

Course Designer

From UGC SYLLABUS