ABILITY ENHANCEMENT COMPULSORY COURSE -II(AECC-II)

CYBER SECURITY

(2026 - 2027 Onwards)

Semester I	Internal Marks: 100		External Marks: -	
COURSE CODE	**COURSE TITLE**	**CATEGORY**	**Hrs /Week**	**CREDITS**
26UGCS	**CYBER SECURITY**	**ABILITY ENHANCEMENT COMPULSORY COURSE**	**2**	**2**

Course Objectives

- 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 analyse and evaluate the basic security aspects related to Computer and Mobiles

S. No.	Course Features	Relevance Status
1.	Course emphasis on Employability/ Entrepreneurship/Skill Development	Employability, Skill Development
2.	Course integrates cross cutting issues relevant to Professional Ethics/Gender sensitization/ Environment and Sustainability/ Human Values/Indian Knowledge System	Professional Ethics, Gender Sensitization, Human Values
3.	Course relevant to Local/Regional/National/ Global needs	Local, Regional, National, Global needs
4.	Course focus on Sustainable Developmental Goals	SDG 4, 5, 16

Course Outcomes

Course Outcome and Cognitive Level Mapping

CO Number	CO Statement On the successful completion of the course, students will be able to	Cognitive Level
CO1	Outline the concept of cyber security, cyber-crime, cyber law and the issues and challenges	K1
CO2	Develop deeper understanding of cyber-crimes, their nature, and legal remedies using case studies	K2
CO3	Apply various privacy and security measures in social media and online payments	K3
CO4	Analyse tools and techniques used for cyber security	K4
CO5	Evaluate security aspects of Computer, Mobiles and other digital devices	K5

Mapping of CO with PO and PSO

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

UNIT	CONTENT	HOURS	COs	COGNITIVE LEVEL
I	**Introduction to Cyber Security:** Defining Cyberspace and Overview of Computer and Web technology - Communication and web technology - Internet infrastructure for data transfer and governance - Issues and challenges of cyber security.	6	CO1, CO2, CO3, CO4, CO5	K1, K2, K3, K4, K5
II	**Cyber Crime :** Cyber crime targeting computers and mobiles - cyber crime against women and children - financial frauds- social engineering attacks - zero day and zero click attacks.	6	CO1, CO2, CO3, CO4, CO5	K1, K2, K3, K4, K5
III	**Social Media Overview and Security:** Introduction to Social networks - Types of Social Media - Social media monitoring – Hashtag - Viral content - Social media marketing .	6	CO1, CO2, CO3, CO4, CO5	K1, K2, K3, K4, K5
IV	**E-Commerce :** Definition of E- Commerce - Elements of E-Commerce security - ECommerce threats - E-Commerce security best practices.	6	CO1, CO2, CO3, CO4, CO5	K1, K2, K3, K4, K5
V	**Digital Payments:** Unified Payment Interface (UPI) - Digital payments related common frauds and preventive measures - RBI guidelines on digital payments and customer protection in unauthorized banking transactions.	6	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.	-	CO1, CO2, CO3, CO4, CO5	K1, K2, K3, K4, K5

Reference Books

1. Sunit Belapure and Nina Godbole, (2011). *Cyber Security Understanding Cyber Crimes*,
2. Henry A. Oliver, (2015). *Security in the Digital Age: Social Media Security Threats and Vulnerabilities* Create Space Independent Publishing Platform, Pearson.
3. Krishna Kumar, (2011). *Cyber Laws: Intellectual Property & E-Commerce Security*, Dominant Publishers.
4. Eric Cole, Ronald Krutz, (2011). *Network Security Bible*, Wiley India Pvt. Ltd, 2nd Edition.
5. R. C Mishra, (2010). *Cyber Crime: Impact on the New Millennium*, Authors Press. Edition 2010.

Web References

1. **https://www.udacity.com/course/intro-to-cybersecurity-nanodegree--nd545**
2. **https://www.techtarget.com/searchsecurity/definition/cybersecurity**
3. **https://www.financemagnates.com/fintech/payments/the-evolution-of-digital-payments-and-ecommerce/**
4. **https://www.cyberralegalservices.com/casestudies.php**
5. **https://www.vidhikarya.com/legal-blog/cyber-crime-and-cyber-law-in-india**

Pedagogy

Power Point Presentations, Group Discussions, Seminar, Quiz, Assignment.

Course Designers

1. Dr. R. Divya
2. Ms. A. Gowri Shankari

Ability Enhancement Compulsory Course II (AECC-II)

CYBER SYCURITY (26UGCS)

Assessment Rubrics for 100 Marks

1.Seminar/Paper Presentation **- 20 marks**

2.Narration of stories describing different types of cyber-attack incidents **- 20 Marks**

3.Video making about cyber-attacks and different types of cyberattack incidents using social engineering and how to avoid (minimum 5 minutes) **- 20 Marks**

4.VIVA VOCE **- 40 Marks**

S.NO	Rubrics for VIVA VOCE	MARKS
1	Subject content • Quality – what is in or out/ depth; • Quantity – coverage of the subject/ breadth; • Accuracy of information in terms of subject matter	20
2	Command of the subject: • Response to questions • Conceptual understanding	10
3	Mannerism, interest generated: • Engaging – eye contact; • Audible	10
Total		**40**

There will be no End Semester Examination for this course. The subject teacher will make an assessment of the students' performance based on the above-mentioned components and an internal VIVA VOCE will be conducted by the subject teacher and marks will be awarded and submitted to COE in the prescribed format specified by the Controller of Examinations with the approval of the Head of the respective Departments.