23CSSDL102

Cyber Security

Offered to: ALL UG PROGRAMS Semester: II

Year of Introduction: 2023 – 2024 Year of Offering: 2023 – 2024 Course Type: Skill Development - Theory Hours: 30 Credits: 2

Course Description:

This course aims to give students a fundamental understanding regarding various cyberattacks and their countermeasures.

Course Objectives:

- 1. To educate students about various types of security attacks and improve their personal cyber security.
- 2. To educate students about the importance of passwords and handling passwords along with avoiding social engineering.
- 3.To educate students about handling security incidents, data backup and recovery. This course also aims to give an overview of career opportunities in cyber security.

Learning Outcomes:

Course Outcome	Upon successful completion of the course, a student will be able to:	Program Outcome
CO1	Develop an understanding of cybercrimes and various legal perspectives involved.	PO6
CO2	Develop a security model to handle mobile, wireless devices and related security issues of an organization.	PO6
CO3	Use the cybercrime tools and methods in solving real world problems	PO6

UNIT - I: 8 hrs

Introduction to Cybercrime: Introduction, Cybercrime: Definition and origins of the word, Cybercrime and Information Security, who are cyber criminals? classifications of cybercrimes, cybercrime: the legal perspectives, an Indian perspective, cybercrime and the Indian IT Act 2000, a Global perspective on Cybercrimes.

UNIT-II: 12hrs

Cybercrime-Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Authentication Service Security, Attacks on Mobile/Cell Phones.

Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile Devices-Related Security Issues, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.

UNIT-III: 10hrs

Tools and Methods Used in Cybercrime: Password Cracking, key loggers and Spywares, virus and worms, Trojan Horses and Backdoors, Steganography, attacks on wireless networks, Phishing and Identity Theft: Introduction, Phishing, Identity Theft (ID Theft).

Text Books:

- 1. Mark Rhodes, Ousley, Information Security, 1st Edition, MGH, 2013.
- **2.** Nina Godbole and SunitBelpure Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, 1st Edition Publication Wiley, 2011.

Activities Planned:

- 1. Identify a user of internet, label him as a cybercriminal or not.
- 2. Checklist for reporting cybercrime at Cybercrime Police Station.
- 3. Checklist for reporting cybercrime online.
- 4. Reporting phishing emails.
- 5. Demonstration of email phishing attack and preventive measures.
- 6. Checklist for secure net banking

Prescribed Text Book: Cyber Security for Dummies, Joseph Steinberg, Wiley

Reference Books: Cyber Security Essentials, Charles J Brooks, Christopher Grow,

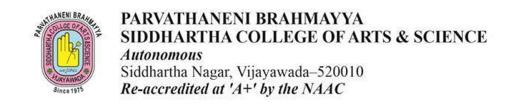
Philip Craig. Wiley

Course Delivery method: Face-to-face / Blended

Course has focus on: Skill Development

Co-curricular Activities: Certification Courses, Quiz, Seminars, Group Discussions, Creating Cyber Security awareness among general public and other students by organizing campaigns.

(a)(a)(a)(a)



MODEL PAPER FOR SEM END THEORY EXAMINATION

23CSSDL104: Cyber Security

Offered to : All UG Programs Semester: II Max. Marks : 50 (CIA: 15 + SEE: 35) Hrs/Week: 2

Time:2Hours

SECTION A

Answer **ANY THREE** questions

 $3 \times 5 = 15 \text{ Marks}$

- 1. Explain Cybercrime and its types. (CO1, L1)
- 2. Write about classification of Cybercrime.(CO1, L6)
- 3. Summarize Mobile devices. (CO2, L2)
- 4. Explain about Password Cracking. (CO3, L1)

SECTION B

Answer **ANY TWO** questions

 $2 \times 10 = 30 \text{ Marks}$

- 6. Explain about Cybercrime and Cybercriminal. (CO1, L1)
- 7. Summarize Cyber-attacks. (CO2, L2)
- 8. Categorize and Explain Tools and Methods Used in Cybercrime. (CO3, L4)

(a)(a)(a)(a)