CIS 183C : INTRODUCTION TO CYBERSECURITY

Transcript title

Intro to Cybersecurity

Credits

4

Grading mode

Standard letter grades

Total contact hours

50

Lecture hours

30

Other hours

20

Recommended preparation

CIS 124 or equivalent computer skills.

Course Description

Introduces students to the critical concepts and principles that surround cybersecurity. Functions as a survey of major topics in the cybersecurity field but also introduces a range of interrelated industry careers, vocabulary, tools, frameworks, and methodologies. Requires students to sign a “White Hat” agreement to participate in this course.

Course learning outcomes

1. Define the context and importance of core principles of cybersecurity.
2. Properly and intentionally use the vocabulary associated with cybersecurity.
3. Evaluate various security systems, practices, and frameworks for overall effectiveness, usability, and feasibility.
4. Work with cybersecurity tools commonly used in the field of ethical hacking.

Content outline

1. Introduction to Cybersecurity
2. Malware and Cyber Attacks
3. Password and Authentication
4. Social Engineering
5. Cryptography
6. Open Source Intelligence (OSINT)
7. Privacy
8. Network and Endpoint Security
9. Risk and Compliance
10. Next Steps

Required materials

Reliable Internet access for web-based e-books and learning resources is required. As well as a modern computer, Windows OS is preferred, able to run multiple virtual machines.