CYBR C101: INTRODUCTION TO CYBERSECURITY

Item	Value
Curriculum Committee Approval Date	10/27/2023
Top Code	070810 - Computer Networking
Units	3 Total Units
Hours	68 Total Hours (Lecture Hours 54; Lab Hours 14)
Total Outside of Class Hours	0
Course Credit Status	Credit: Degree Applicable (D)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	No
Open Entry/Open Exit	No
Grading Policy	Standard Letter (S), • Pass/No Pass (B)

Course Description

This course introduces the foundational concepts of cybersecurity, including social engineering, cybersecurity resilience, and cyber threats. The principles and structure of confidentiality, integrity, and availability are surveyed to provide a foundation for further study of cybersecurity. This course covers data privacy and security, system security, and personal security factors to examine the nature and roles of organizational security policies and risk management processes. Suitable for majors and non-majors interested in cybersecurity tools, techniques, and practices. Security exercises help students develop skills to prepare for careers such as Information Security Analyst, Cyber Crime Analyst, and Incident and Intrusion Analyst. ADVISORY: IT C104 or CIS C111. Transfer Credit: CSU.

Course Level Student Learning Outcome(s)

1. Evaluate and recommend practical solutions to reduce the risk associated with common social engineering attacks.
2. Assess cyber threats in a given business scenario to make recommendations for reducing risk to improve organizational security.
3. Create a security awareness training campaign for a community organization, a private company, a government department, or an academic institution.

Course Objectives

- 1. Describe foundational cybersecurity terms and history.
- 2. Explain how to find resources that provide relevant, up-to-date global threats.
- 3. Define types of malware, viruses, and ransomware along with common countermeasures.
- 4. Describe cyber principles as related to personal security and modern cyber laws.
- 5. Evaluate common social engineering tactics, techniques, and procedures.
- 6. Enumerate and explain various types of cybersecurity from personal security to critical infrastructure security.
- 7. Share current examples of government initiatives that support cyber resilience in industry and government organizations.
- 8. Associate cybersecurity careers with various types of cybersecurity practices and cyberattacks.
- 9. Compare and contrast the content and commerce on the public World Wide Web with the Dark Web.
- 10. Facilitate the development of recommendations for personal security improvements.

Lecture Content

Basics of Cybersecurity Threat Landscape Malware, Viruses, and Ransomware Cyber Principles, Integrity, and Ethics Social Engineering Personal Security Physical Security Organizational Security Data Security and Privacy System Security Network Security Endpoint and Mobile Device Security Cloud, IoT, and Medical Device Security Critical Infrastructure Security Vendor/Third-Party Security eCrime and the Dark Web Cyber Resilience and Government Initiatives Cybersecurity Careers Improving Your Security

Lab Content

Analyze a data privacy policy and identify privacy risks based on technical aspects of data collection, sharing, and renting/leasing to third-party providers Configure a router to understand the risks to security and privacy Crack passwords to recognize the risks to security and privacy Evaluate physical security to minimize data security risks Review vendor security policies to compare to organizational security policies Use social engineering techniques to develop an attack scenario to evaluate effectiveness and likelihood of success

Method(s) of Instruction

- Lecture (02)
- DE Live Online Lecture (02S)
- DE Online Lecture (02X)
- Lab (04)
- DE Live Online Lab (04S)
- DE Online Lab (04X)

Instructional Techniques

This course will utilize a combination of lecture, remote virtual machine lab assignments, system simulators, classroom discussion with student interactions, problem-solving techniques, quizzes, exams, and troubleshooting assignments to achieve the goals and objectives of this course. All instructional methods are consistent across all modalities.

Reading Assignments

Read open educational resource materials Read journal articles and corporate reports Read news articles Read interactive career websites Read privacy policies

Writing Assignments

Develop a security awareness training campaign Create a security awareness presentation for a select target audience Create a social media post to increase public awareness about cybersecurity Write short essays about course topics

Out-of-class Assignments

Conduct online research to find preventative measures for social engineering attacks Conduct online research to locate recommendations and suggestions for security awareness training Lab assignments

Demonstration of Critical Thinking

Students will write technical reports based on the instructions provided in the remote lab simulators or case scenarios to demonstrate the application of critical thinking.

Required Writing, Problem Solving, Skills Demonstration

Configure various security software tools. Use remote lab environment to demonstrate mitigation techniques to assess vulnerabilities in a computer network environment.

Eligible Disciplines

Computer information systems (computer network installation, microcomputer ...: Any bachelor's degree and two years of professional experience, or any associate degree and six years of professional experience. Computer service technology: Any bachelor's degree and two years of professional experience, or any associate degree and six years of professional experience.

Textbooks Resources

1. Required Whitman, M.; Mattord, H. Principles of Information Security, 7th ed. Boston: Cengage, 2022 2. Required Ciampa, M. Security Awareness: Applying Practical Cybersecurity in Your World, 6th ed. Boston: Cengage, 2024 Rationale: -

Other Resources

1. Coastline Library 2. White papers, security reports, and articles are available at no charge to all students at multiple sites as recommended by the instructor. 3. McCarthy, L. Own Your Space, 1st ed. Microsoft, 2011 Open educational resource