

**Syllabus for
Computer Security Fundamentals, 5/E
2026-2027**

***INSTRUCTOR'S NAME:* Faye Jackson**

***OFFICE:* B-128**

***E-MAIL:* fjackson@wilcoacc.org**

***COURSE CODE:* CYBIT 150**

***COURSE TITLE:* Computer Security Fundamentals**

***PREREQUISITE:* N/A**

***CREDITS:* (3) College Credits**

COURSE DESCRIPTION:

This introductory-level course provides an overview of computer security topics, with a focus on understanding the most common threat types and implementing basic protection systems for device, data, and network protection.

COURSE OBJECTIVES:

Upon successful completion of this course, students should demonstrate proficiency in the following areas:

- Cyberstalking, fraud, and abuse
- DoS attacks
- Malware
- Hacking techniques
- Industrial espionage in cyberspace
- Encryption
- Computer security technology
- Security policies
- Network scanning and vulnerability scanning
- Cyber terrorism and information warfare
- Locating information relevant to an investigation online
- Forensics
- Cybersecurity engineering

REQUIRED COURSE MATERIALS:

Dr. Chuck Easttom, *Computer Security Fundamentals, 5th Edition*. Pearson Education, 2023.
ISBN-13: 978-0-13-798478-7
ISBN-10: 0-13-798478-2

REQUIRED SUPPLEMENTARY MATERIALS:

SUGGESTED READINGS:

ANNOTATED LIST OF ELECTRONIC RESOURCES

METHOD OF INSTRUCTION:

This class includes lecture and class discussion, demonstrations, and hands-on practice. Student participation is encouraged and mandatory in required assignments and practical demonstrations, including both individual and group tasks.

INSTRUCTIONAL MATERIALS:

- Computer (desktop or laptop) and Internet access
- Digital projector and connected laptop (instructor)
- Instructor materials to accompany textbook (instructor)

STUDENT EXPECTATIONS:

- Read all course materials, including the syllabus and description of the grading and testing systems to be used in the course.
- Attend every class session and complete all assignments on time.
- Participate in all classroom learning activities.
- Interact respectfully with faculty, staff, and fellow students.
- Refrain from all academic misconduct.
- Avoid situations that give the appearance of misconduct.
- Report any observed academic misconduct.

GRADING SYSTEM:

The grading system is as follows:

Graded Element	Maximum Points
Review Questions (15 chapters @ 10 points each)	150
Exercises (69 @ 10 points each)*	690
Projects (40 @ 10 points each)**	400
Class participation	150
Total	1390

* Note: When more than 3 exercises are available for a week, instructor should choose 3.

** Note: When more than one 1 project is available for a week, instructor should choose 1.

Grade Scale (Percentage)			
A+	98-100	C+	78-79
A	93-97	C	73-77
A-	90-92	C-	70-72

B+	88-89	D+	68-69
B	83-87	D	63-67
B-	80-82	D-	60-62

MAKEUP POLICY:

Any graded element may possibly be turned in one day per an Excused absence.

CLASSROOM POLICIES

- Cell phone ringers must be off and put away in the phone holder, and may NOT be used in class, no matter how briefly. Phones may be used in the main office area.
- Computers may not be used for any non-related course work during class time.
- The use of unapproved Artificial Intelligence is forbidden for any and all assignments.

ABSENCES

To succeed in the course, students must attend and participate in each class session. If you miss a session, it is your responsibility to learn any material missed.

ACADEMIC INTEGRITY / CHEATING

Any form of cheating on an assignment, homework, lab, or test will result in both a zero score for the assignment and a one-letter grade penalty in the course.

Plagiarism is the use of someone else's words, ideas, or data without giving credit to the original author. Plagiarism is a form of cheating.

If you are confused as to the difference between helping each other (which is encouraged) and cheating (which will not be tolerated), ask your instructor.

Acceptable	Cheating
Including a brief quote from a web page with the source cited.	Copying entire pages or paragraphs and republishing it as your own.
Using graphics from a free clip art or graphic site.	Using someone else's graphics without permission.
Discussing an assignment with another student.	Copying another student's work or file.
Looking at online sources or asking for a classmate's help to figure out what to do.	Duplicating a classmate's lab answers as your own, without performing the lab activity yourself.

If you assist someone else in cheating, you can also be charged with cheating yourself. This can include giving another student access to your computer account, negligently permitting another student to access your account, or posting answer keys where others can access them. Protect your account as if your academic career depends on it!

WEEKLY COURSE OUTLINE

Week	Topics	Chapter Readings	Assignments	Activities and Testing
1	Introduction to Computer Security • How Seriously Should You Take Threats to Network Security? • Identifying Types of Threats • Assessing the Likelihood of an Attack on Your Network • Basic Security Terminology • Concepts and Approaches • How Do Legal Issues Impact Network Security? • Online Security Resources	Chapter 1	Read pp. 2-27 Review questions 1-20, pp. 27-30	Discussion: Case Study, p. 32 Exercises 1.1 – 1.5 Projects 1.1 – 1.3
2	Networks and the Internet • Network Basics • How the Internet Works • History of the Internet • Basic Network Utilities • Other Network Devices • Advanced Network Communications Topics • Cloud Computing	Chapter 2	Read pp. 34-65 Review questions 1-25, pp. 65-69	Exercises 2.1 – 2.5 Projects 2.1 – 2.3
3	Cyber Stalking, Fraud, and Abuse • How Internet Fraud Works • Identity Theft • Cyber Stalking • Protecting Yourself Against Cybercrime	Chapter 3	Read pp. 74-99 Review questions 1-24 pp. 99-103	Discussion: Case Study, p. 105 Exercises 3.1 and 3.2 Projects 3.1 – 3.3 Quiz #3
4	Denial of Service Attacks • DoS Attacks • Illustrating an Attack • Common Tools Used for DoS Attacks • DoS Weaknesses • Specific DoS Attacks	Chapter 4	Read pp. 106-123 Review questions 1-20 pp. 123-126	Discussion: Case Study, p. 129 Exercises 4.1 – 4.4 Projects 4.1 – 4.3

	• Real-World Examples of DoS Attacks • How to Defend Against DoS Attacks			
5	Malware • Viruses • Trojan Horses • The Buffer-Overflow Attack • Spyware • Other Forms of Malware • Detecting and Eliminating Viruses and Spyware	Chapter 5	Read pp. 130-159 Review questions 1-20, pp. 159-163	Discussion: Case Study, p. 165 Exercises 5.1 – 5.5 Projects 5.1 – 5.3
6	Techniques Used by Hackers • Basic Terminology • The Reconnaissance Phase • Actual Attacks • Malware Creation • Penetration Testing • The Dark Web	Chapter 6	Read pp. 166 - 194 Review questions 1-15, pp 194-197	Discussion: Case Study, p. 198 Exercises 6.1 – 6.4 Projects 6.1 and 6.2
7	Industrial Espionage in Cyberspace • What Is Industrial Espionage? • Information as an Asset • Real-World Examples of Industrial Espionage • How Does Espionage Occur? • Protecting Against Industrial Espionage • Trade Secrets • The Industrial Espionage Act • Spear Phishing	Chapter 7	Read pp. 200-220 Review questions 1-15, pp. 220-223	Discussion: Case Study, p. 225 Exercises 7.1 – 7.5 Projects 7.1 – 7.3
8	Encryption • Cryptography Basics • History of Encryption • Modern Cryptography Methods • Public Key (Asymmetric) Encryption • PGP	Chapter 8	Read pp. 226-261 Review questions 1-18, pp. 261-264	Discussion: Case Study, p. 266 Exercises 8.1 – 8.4 Projects 8.1 – 8.3

	• Legitimate Versus Fraudulent Encryption Methods • Digital Signatures • Hashing • MAC and HMAC • Steganography • Cryptanalysis • Cryptography Used on the Internet • Quantum Computing Cryptography			
9	Computer Security Technology • Virus Scanners • Firewalls • Antispyware • IDSs • Digital Certificates • SSL/TLS • Virtual Private Networks • Wi-Fi Security	Chapter 9	Read pp. 268-299 Review questions 1-15, pp. 299-301	Discussion: Case Study, p. 303 Exercises 9.1 – 9.5 Projects 9.1 – 9.3
10	Security Policies • What Is a Policy? • Important Standards • Defining User Policies • Defining System Administration Policies • Security Breaches • Defining Access Control • Development Policies • Standards, Guidelines, and Procedures • Disaster Recovery • Zero Trust • Important Laws	Chapter 10	Read pp. 304-330 Review questions 1-15, pp. 330-333	Discussion: Case Study, p. 335 Exercises 10.1 – 10.6 Projects 10.1 – 10.3
11 & 12	Network Scanning and Vulnerability Scanning • Basics of Assessing a System • Securing Computer Systems • Scanning Your Network • Testing and Scanning Standards • Getting Professional Help	Chapter 11	Read pp. 336-369 Review questions 1-20, pp. 369-373	Discussion: Case Study, p. 376 Exercises 11.1 – 11.9 Projects 11.1 – 11.5

13	Cyber Terrorism and Information Warfare • Actual Cases of Cyber Terrorism • Weapons of Cyber Warfare • Economic Attacks • Military Operations Attacks • General Attacks • Supervisory Control and Data Acquisitions (SCADA) • Information Warfare • Actual Cases of Cyber Terrorism • Future Trends • Defense Against Cyber Terrorism • Terrorist Recruiting and Communication • TOR and the Dark Web	Chapter 12	Read pp. 378-402 Review questions 1-14, pp. 402-404	Discussion: Case Study, p. 406 Exercises 12.1 – 12.5 Projects 12.1 – 12.3
14	Cyber Detective • General Searches • Company Searches • Court Records and Criminal Checks • Usenet • Google • Maltego	Chapter 13	Read pp. 408-421 Review questions 1-15, pp. 421-423	Discussion: Case Study, p. 425 Exercises 13.1 – 13.5 Projects 13.1 – 13.3
15	Introduction to Forensics • General Guidelines • Finding Evidence on a PC • Finding Evidence in System Logs • Getting Back Deleted Files • Operating System Utilities • The Windows Registry • Mobile Forensics: Cell Phone Concepts • The Need for Forensic Certification • Expert Witnesses • Additional Types of Forensics	Chapter 14	Read pp. 426-463 Review questions 1-9, pp. 463-464	Exercises 14.1 – 14.3

16	Cybersecurity Engineering • Defining Cybersecurity Engineering • Standards • SecML	Chapter 15	Read pp. 466-491 Review questions 1-10, pp. 491-493	Exercises 15.1 and 15.2
----	---	------------	--	-------------------------

Note: This course outline is subject to change.