ITC 300 – Security in a Digital Society

Fall 2024

Instructor	Garrett Poppe	**E-Mail**	gpoppe@csudh.edu
Classroom	Online	**Class Time**	Online
Office	Online	**Office Hours**	Online by Appointment
Phone	(310) 243-3398	**URL**	*http://csc.csudh.edu*

COURSE DESCRIPTION

This course provides students with an understanding of digital threats and how to utilize a computer securely and as a valuable service to business and personal life. Students will learn security across several domains including data privacy, e-commerce, social media, cloud services, and applications in a digital society.

TEXTBOOKS

No textbooks are required.

COURSE GOALS

The primary goal of this course is to teach students to analyze the vulnerabilities and related solutions in the areas of data privacy, e-commerce, social media, cloud services, and applications. The course presents solutions ranging from safe browsing practices to cryptography and its function to online applications. Federal Government and Industry guidance on Information Assurance and Cybersecurity are introduced.

COURSE OUTCOMES

Upon completion of the course the students will be able to:

1. Effectively use the Vocabulary associated with cybersecurity.
2. Define the principles of cybersecurity.
3. Describe the fundamental concepts of the cybersecurity discipline and use to supply system security.
4. Describe potential system attacks and the actors that might perform them.
5. Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks.
6. Describe proper measures to be taken should a system compromise occur.
7. Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies.
8. Analyze common security failures and find specific design principles that have been violated.
9. Given a specific scenario, find the design principles involved or needed.

10. Understand the interaction between security and system usability and the importance for minimizing the effects of security mechanisms.
11. Describe the hardware components of modern computing environments and their individual functions.
12. Describe the basic security implications of modern computing environments.
13. Understand the Federal, State and Local Cyber Defense partners/structures.

AMERICANS WITH DISABILITIES ACT

CSUDH adheres to all applicable federal, state, and local laws, regulations, and guidelines with respect to providing reasonable accommodations for students with temporary and permanent disabilities. If you have a disability that may adversely affect your work in this class, I encourage you to register with Disabled Student Services (DSS) and to talk with me about how I can best help you. All disclosures of disabilities will be kept strictly confidential. NOTE: no accommodation can be made until you register with the DSS. For information call (310) 243-3660 or to use the Telecommunications Device for the Deaf, call (310) 243-2028 or go to: https://www.csudh.edu/sdrc/

COMPUTER INFORMATION LITERACY EXPECTATIONS

It is expected that students will:

1. *Use Microsoft Word for word processing unless otherwise approved by the instructor.*
2. *Be familiar with using email as a communication tool and check your official campus email account at least every other day.*
3. *Be able to access websites and online course materials which may require the use of multiple web browsers.*
4. *Use the library databases to find articles, journals, books, databases, and other materials.*
5. *Be able to use Zoom and Canvas.*
6. *Have regular access to a computer and internet access for the term of this course.*

ACADEMIC INTEGRITY

Academic integrity is of vital importance in this and every other course at CSUDH. You are obliged to consult the proper sections of the University Catalog and obey all rules and regulations imposed by the University relevant to its lawful missions, processes, and functions. ***All work turned in by a student for a grade must be the students' own work.*** Plagiarism and cheating (e.g., stealing or copying the work of others and turning it in as your own) will not be tolerated, and will be dealt with according to university policy. The consequences for being caught plagiarizing or cheating range from a minimum of a zero grade for the work you plagiarized or cheated on, to being dropped from the course or expelled from the University.

COURSE POLICIES

- Deliverables (Class Assignments, Projects) submitted late are not accepted.

- Deliverables (Class Assignments, Projects) not submitted before the end of the final class will earn 0%.
- Any exceptional, non-academic circumstances need to be discussed with the instructor as soon as they arise, prior to the due date of the deliverable. At the time of the discussion, NO make-up work will be assigned.

The instructor reserves the right not to award credit for deliverables that are incomplete. Partial credit is awarded at the instructor's discretion, and only for work which merits such an award. Assignments that are incomplete or incongruous with the specifications may be returned to the student.

MIDTERM & FINAL EXAM

Midterm Exam 1 is during the sixth week of the class.

Midterm Exam 2 is during the twelfth week of the class, and the date for the final exam is based on the final examination schedule printed in the campus Class Schedule.

No makeup or early exams will be administered.

GRADES

Score	Grade	Score	Grade
96-100	A	90-95	A-
87-89	B+	83-86	B
80-82	B-	77-79	C+
73-76	C	70-72	C-
67-69	D+	63-66	D
0-62	F		

GRADING:

The weighting of the coursework is listed below:

Exam 1	**15%**
Exam 2	**15%**
Final Exam	**15%**
Labs and Quizzes	**55%**
Total:	**100%**

TOPIC OUTLINE (Will be conducted according to the following. However, the schedule of the topics schedule or timetable may be varying slightly)

Tentative Course Schedule

Week #	**Date**	**Topic**	***Reading Assignment/Lab***
Week 1	8/26/24	Course introduction and requirements. Overview of References and Blackboard/Canvas.	Lab #1
Week 2	9/02/24	Need for Security. Potential system attacks and the actors behind them.	Lab #2
Week 3	9/09/24	Cybersecurity terms and principles.	Lab #3
Week 4	9/16/24	Planning for security. Safe practices and policies.	Lab #4
Week 5	9/23/24	Physical and local computer security.	Labs #5
Week 6	9/30/24	**Exam 1**	Lab #1-5
Week 7	10/07/24	Encryption and data privacy.	Lab #6
Week 8	10/14/24	Virtual Machines (VM).	Lab #7
Week 9	10/21/24	E-commerce and cloud computing.	Lab #8
Week 10	10/28/24	Firewalls, VPNs, and network devices.	Lab #9
Week 11	11/04/24	Implementing information security.	Lab #10
Week 12	11/11/24	**Exam 2**	Lab #6-10
Week 13	11/18/24	Security policies and personnel.	Lab #11
Week 14	11/25/24	Legal, ethical, and professional issues in information security.	Lab #12
Week 15	12/02/24	Information security maintenance.	Lab #13
Week 16	12/09/24	**Final Exam Week**	**Final Exam**