CSCI 102 – Computer FUNdamentals for Cyber Security
Spring 2024

Instructor:	Dr. Suzanne Mello-Stark
Email:	smellostark@ric.edu (best way to reach me)
Office Location:	Zoom Room/Alger 235
Office Hours:	Tuesday Noon – 2pm or by Zoom appointment
Course Website:	Blackboard
Class Days/Times:	Asynchronous (no meeting times)
Classroom:	Asynchronous (no classroom)
Prerequisites:	Math competency

No Textbooks Required

Course Description

This course provides the technical background necessary for non-computer science majors to study and master cyber security challenges. This course significantly improves students' ability to understand the digital world in which they live. It is a valuable course for any student wishing to pursue a career in cyber security or any other technical field.

At the end of this course, students will be able to:

- Demonstrate understanding of key concepts in computer architecture such as bits/bytes, CPUs, processes, memory, and storage management.
- Demonstrate an understanding of how the Internet works and its most widely used protocols.
- Define the major terms in networking such as WAN/LAN, TCP/IP, OSI, VPNs, Firewalls, and wireless protocols.
- Show mastery in database concepts and basic SQL commands.

Assignments and Grading Policy

Activities	40%
Discussions	20%
Quizzes (6)	20%
Projects (2)	20%

Course Approach

This course is asynchronous which means students have flexibility to schedule their time wisely and complete all assignments on time. Each week a new page will open. This page will contain the objectives for the week and instructions, the week's modules, a discussion, and a bi-weekly quiz. Students have one week to complete the material unless otherwise indicated.

There are 2 modules per week on average. Each module may have readings, videos and activities to help you master the material. For the best chance for success, complete at least one module per day, plan on visiting the discussion at least 3 days a week and leave

time to study for and take the quiz by the end of the week.

Two projects will be assigned in this course. The first project is a poster on an emergent topic. The second is to interview a cyber security professional in the field.

All activities and discussions are due on Mondays in Blackboard by 11:55 pm. I also open the next week on Fridays. This means you usually have two weekends to complete the assignments. Plenty of time for an organized student to master the material stress free at their own pace!

If you had an unusually busy week, there is a two-day grace period on assignments. After two days, 10 points will be deducted from the assignment if the instructor was not contacted with a valid excuse **prior** to the assignment being due. So, communication is key!

Discussions are how we communicate and maintain our community. Please take a close look at the discussion rubric in the course so you don't lose points. Discussions will not be accepted late and close promptly. You must do them in the week they are due with no chance of make-up.

Week	Date	Topics
1	Jan 16 - 19	Ethics Module 0: Ethics Module 1: Hackers Discussion 1 – Welcome!
2	Jan 22 - 26	Cyber Security Awareness Module 2: Cyberbullying Module 3: How to Stay Safe Online Module 4: Passwords Discussion 2 – Impactful Hacks
3	Jan 29 – Feb 2 Last Day to add/drop – Jan 29	Security Basics Module 5: Cyber Security Principles and the CIA Triad Module 6: Viruses and Worms Project 1 – Topic Due Discussion 3 – Pick your Poster Topic Quiz 1 on Week 1 and 2
4	Feb 5 - 9	Security Basics Module 7: Security Threat Analysis Module 8: Bits and Bytes Project 1 – Reading List Activity Due Discussion 4 – Class Cyberbullying Survey Results
5	Feb 12 - 16	Phishing and Malware Module 9: Phishing Quiz Module 10: Malware Types Discussion 5 – NIST Importance to Cyber Quiz 2 on Week 3 and 4
6	Feb 19 - 23	Enigma Machine and Steganography Module 11: Steganography Project 1 – Full Bibliography Due Discussion 6 - Privacy

7	Feb 26 – Mar 1	Module 12: Public Key Infrastructure Discussion 7 – Applications of Cryptography Quiz 3 on Week 5 and 6
8	Mar 4-8	How the Internet Works Module 13: WWW and its Protocols Discussion 8 - Malinformation
9	Mar 11 – 15 Spring Break	Quiet Week Discussion 9 (not graded – just for fun or questions)
10	Mar 18 - 22 Mar 20 – Midterm Grades Due	**Project 1 – Posters – Due March 20** Poster Week! Discussion 10 – Posters Quiz 4 on Week 7 and 8
11	Mar 25- Mar 29	How the Internet Works Module 14: IoT Devices Module 15: Social Media Discussion 11 – Career Research Project 2 – Name of Interviewee Due
12	Apr 1– 5 Apr 3 – last day to drop with W	Networking Basics Module 16: Packet Sniffing and Spoofing Discussion 12 – Virtual Machines Project 2 – List of Interview Questions due
13	Apr 8 - 12	Networking Basics Module 17: How TCP/IP works Module 18: Domain Name Servers Discussion 13 – NIST Framework and Documents Quiz 5 on Week 11 and 12

14	Apr 22 - 26	Database Basics Module 19: SQL Tutorial Module 20: SQL Injection Activity Module 21: Tables, Keys and Queries Discussion 14 –Cybersecurity Mindset and Final Thoughts Project 2 – Interview Conducted Quiz 6 on Week 13 and 14
15	Apr 29 Last day of term April 29	**Project 2 – Interview - Due April 29th**

The above schedule, policies, procedures, and assignments are subject to change in the event of extenuating circumstances, by mutual agreement, and/or to ensure better student learning.

My Policies

Assessment and Feedback Plan

Students can expect a response on email /discussions within 24 hours Monday-Friday. Assignments will be graded within one week of when assignments are due.

Rhode Island College Course Policies

Academic Integrity

All work submitted for credit must be your own. Plagiarism is cheating and will be dealt with accordingly. You may not share your solutions to homework questions/coding projects with others. Students who violate college rules are subject to disciplinary penalties, including the possibility of failure or removal from the course, disciplinary probation, and/or dismissal from the college. For more information, please read Chapter 3.9, Academic Standards, in the College Handbook.

Late Withdrawals

I cannot grant any late withdrawals in this class. The last day to drop the class with a W is **April 3, 2024**. Please make an appointment to see me if you are in danger of failing the course at this time.

Students with Disabilities

If you need course adaptations or accommodations because of a disability, or if you have medical information to share with me, please make an appointment with me as soon as possible. If you have not already done so, students with disabilities who believe that they may need accommodations in this class are encouraged to contact the Disability Services Center, at (401) 456-2776. You can visit the website at: https://www.ric.edu/department-directory/disability-services-center..

A Special Statement on Ethics, the Law and College Policies

The knowledge presented in this course is in no way intended for use in any illegal capacity and is meant to aid learning and development of cyber security practices and concepts only. Acting ethically and lawfully is the responsibility of every security professional and college student. For more information on what that entails carefully read the Computer Fraud and Abuse Act (CFAA) at https://www.law.cornell.edu/uscode/text/18/1030. This is one of the laws that governs "hacking". Just because you can do it, doesn't mean it's legal. Check out what happened to David Kernell who hacked into Sarah Palin's email https://en.wikipedia.org/wiki/Sarah_Palin_email_hack. Review the college's policies on computing. https://www.ric.edu/department-directory/user-support-services-0/policies-and-guidelines. And review the ACM's guide on Ethics at https://www.acm.org/binaries/content/assets/about/acm-code-of-ethics-and-professional-conduct.pdf as well.