

CYBR C092N: DEVICE SECURITY, PRIVACY, AND CYBER CAREERS

Item	Value
Eff Term	Fall 2026
Curriculum Committee Approval Date	12/05/2025
Top Code	070800 - Computer Infrastructure and Support (CTE)
Units	0 Total Units (Lecture Units 0)
Hours	27 Total Hours (Lecture Hours 27)
Total Outside of Class Hours	0
Total Student Learning Hours	27
Course Credit Status	Noncredit (N)
Material Fee	No
Basic Skills	Not Basic Skills (N)
Repeatable	Yes; Repeat Limit 99
Open Entry/Open Exit	No
Grading Policy	P/NP/SP Non-Credit (D), • Letter Non-Credit (L)

Course Description

This course focuses on securing personal and workplace devices from common threats. Students will learn about software updates, antivirus tools, Wi-Fi protection, mobile device management, and safe cloud storage. The course concludes with an introduction to cybersecurity career pathways and resources for continued learning. Transfer Credit: Not Transferable.

Course Level Student Learning Outcome(s)

1. Implement essential device and network security practices on computers and mobile devices.
2. Apply privacy protection strategies for data stored or shared online.
3. Describe basic cybersecurity roles and identify career exploration resources.

Course Objectives

- 1. Identify key types of digital threats (malware, ransomware, identity theft).
- 2. Demonstrate how to secure operating systems, software, and apps through updates and settings.
- 3. Configure Wi-Fi routers and mobile devices for secure connectivity.
- 4. Understand encryption, backups, and safe cloud storage practices.
- 5. Apply best practices for protecting sensitive or personal data.
- 6. Explore entry-level cybersecurity careers and related certifications (e.g., CompTIA ITF+, Security+).

Lecture Content

- Understanding Cyber Threats and Vulnerabilities
- Securing Your Computer and Mobile Devices

- Safe Use of Wi-Fi and Public Networks
- Antivirus, Firewalls, and System Updates
- Data Backup and Recovery Basics
- Cloud Security and Encryption
- Privacy in the Digital Workplace
- Identity Theft Prevention and Response
- Cybersecurity Career Pathways and Certificates
- Lifelong Learning and Digital Responsibility

Method(s) of Instruction

- Enhanced NC Lect (NC1)
- Live Online Enhanced NC Lect (NC9)
- Online Enhanced NC Lect (NC5)

Instructional Techniques

This course will utilize a combination of lecture, hands-on 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, journal articles and corporate reports, news articles, and interactive career websites.

Writing Assignments

Students write brief explanations of how specific device-security or data-privacy practices protect users in real-life scenarios.

Out-of-class Assignments

Students apply security settings on their own devices, test backup or update procedures, or explore cybersecurity career resources independently.

Methods of Student Evaluation

- Short Quizzes
- Written Assignments
- Projects (Individual/Group)
- Problem Solving Exercises

Demonstration of Critical Thinking

Students demonstrate critical thinking by analyzing real-world device and data-protection scenarios to determine the most effective security settings or practices.

Required Writing, Problem Solving, Skills Demonstration

Students produce short written explanations of security choices, troubleshoot basic device-protection scenarios, and demonstrate skills like configuring updates, backups, or secure connections.

Resources Subscreen

- **Open Education Resource:** Tolboom, R.. *Computer Systems Security: Planning for Success*. (2022).

Eligible Discipline(s)

- Computer information systems (computer network installation, microcomputer technology, computer applications): 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.
- Computer science: Master's degree in computer science or computer engineering OR bachelor's degree in either of the above AND master's degree in mathematics, cybernetics, business administration, accounting or engineering OR bachelor's degree in engineering AND master's degree in cybernetics, engineering mathematics, or business administration OR bachelor's degree in mathematics AND master's degree in cybernetics, engineering mathematics, or business administration OR bachelor's degree in any of the above AND a master's degree in information science, computer information systems, or information systems OR the equivalent. Note: Courses in the use of computer programs for application to a particular discipline may be classified, for the minimum qualification purposes, under the discipline of the application. Master's degree required.