CYBR C091N: ONLINE SAFETY AND DIGITAL CITIZENSHIP

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
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

Students will learn practical skills to navigate the digital world safely and responsibly. Topics include identifying scams and phishing, managing passwords, understanding privacy settings, and protecting personal information on social media, email, and mobile devices. The course also promotes responsible online behavior and awareness of digital footprints. Transfer Credit: Not Transferable.

Course Level Student Learning Outcome(s)

1. Recognize and respond appropriately to online scams, phishing, and social engineering attempts.
2. Apply privacy and security settings on common platforms to safeguard personal data.
3. Demonstrate responsible digital citizenship by managing personal information and online interactions safely.

Course Objectives

- 1. Explain basic cybersecurity terms (e.g., phishing, malware, two-factor authentication).
- 2. Identify safe practices for browsing, downloading, and sharing information online.
- 3. Configure privacy and security settings on social media, browsers, and email accounts.
- 4. Manage passwords securely using recommended tools and practices.
- 5. Describe the concept of a digital footprint and its long-term impact.
- 6. Distinguish between legitimate and fraudulent online communications.

Lecture Content

- Introduction to Cyber Hygiene and Online Safety
- Understanding the Internet Threat Landscape
- Passwords, Authentication, and Account Protection
- Phishing, Scams, and Social Engineering
- Safe Browsing and Secure Communication
- Managing Privacy on Social Media and Apps
- Digital Footprints and Online Reputation
- Protecting Children and Seniors Online
- Reporting Cybercrime and Seeking Help
- Responsible Use of Technology in Work and School

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 complete short reflections or responses analyzing examples of online behavior, privacy choices, or phishing messages.

Out-of-class Assignments

Students review personal devices or accounts to adjust privacy settings, practice password improvements, or identify potential online risks in their daily technology use.

Methods of Student Evaluation

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

Demonstration of Critical Thinking

Students demonstrate critical thinking by evaluating online messages and behaviors to distinguish legitimate communication from deceptive or unsafe interactions.

Required Writing, Problem Solving, Skills Demonstration

Students complete brief written reflections, solve scenario-based online safety problems, and demonstrate skills such as adjusting privacy settings or identifying phishing cues.

Resources Subscreen

- **Open Education Resource:** Bali, M., Blocksidge, K., Caines, A., Levesque, L., Schwartz, M.. *Digital Citizenship Toolkit*. (2019).

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.