**CYBR 201(8339): Web Technologies Essentials: Security and Design**

3 Credits

**Semester:** Fall 2025

**Day/Time:** asynchronous

**Location:** Online

**Instructor:** Crystal Jones-Howe

**Contact:** cjones-howe@albany.edu

**Office Hours:** As requested,

**Office Location:** online

**Office Hour Zoom:** as requested

**Group Project Charter**

**Project Purpose/Justification:**  
The purpose of this group project is to combine web development skills with real-world cybersecurity concepts. Students will research a past or recent cybersecurity incident, analyze its impact, and create a website to present their findings. This project will provide students with hands-on experience in both web development and cybersecurity analysis, enabling them to apply technical skills to real-world problems while enhancing their problem-solving and communication abilities.

**Project Description:**  
In this project, student groups will investigate a significant cybersecurity incident, such as a data breach, hack, or cyber attack. The team will research the event, analyze its impact on various stakeholders, and create a professional website to report on the incident. The website will serve as both an informational resource and a case study that highlights cybersecurity vulnerabilities, response strategies, and lessons learned.

**Goals and Objectives:**

1. Technical Skills Development:
   * Learn how to create a functional, responsive website using HTML, CSS, JavaScript, and web security principles.
   * Integrate multimedia content (such as images, videos, and charts) to effectively communicate findings.
2. Cybersecurity Understanding:
   * Research and analyze a real-world cybersecurity incident.
   * Understand the impact of cybersecurity threats on individuals, businesses, and society.
   * Evaluate response strategies and lessons learned from the incident.
3. Team Collaboration:
   * Work as a group to research, design, and develop the website.
   * Assign roles and responsibilities to leverage each team member's strengths in web development, content creation, and research.
4. Communication and Reporting:
   * Develop effective written and visual content for the website that clearly communicates the incident’s details, impact, and outcomes.
   * Present the website to the class, demonstrating how it informs visitors about the cybersecurity incident.

**Key Deliverables:**

* A research report detailing the cybersecurity incident, its causes, effects, and how it was handled.
* A website that presents the research findings, including interactive elements, visuals, and educational content.
* A presentation where the team showcases their website and explains the incident and their research findings.

**Project Timeline:**  
Week 1-2:

* Team Formation: Group members assigned, and roles defined.
* Research Phase: Select a cybersecurity incident to investigate, gather sources, and start the analysis.

Week 3-5:

* Website Design & Development: Begin designing the website structure and layout using HTML, CSS, and JavaScript.
* Content Creation: Research and write content about the cybersecurity incident for the website.

Week 6-8:

* Website Development: Add interactivity to the site (e.g., JavaScript elements). Implement web security best practices.
* Content Review: Ensure that the website is informative, clear, and engaging. Incorporate visuals like charts, videos, and infographics to support the information.

Week 9-10:

* Final Development & Testing: Finalize website content and design. Ensure the site is fully functional and responsive.
* Team Presentation Preparation: Prepare a presentation to explain the incident and demonstrate the website.

Week 11:

* Website Presentation & Final Report Submission: Present the website at the Albany Showcase. Submit the final report and website link for evaluation.