CIS 115: Introduction to Cybersecurity

Students are introduced to the field of cybersecurity and the communication challenges facing modern businesses in a world of hyper-connectivity. Students will learn about the value of information, types of cyber threats and attack vectors, how to recognize and mitigate cyber threats, and how to deploy common defense mechanisms to safeguard sensitive information. Topics include IT system architectures for processing information, virtualization, access controls, digital forensics, and applicable laws and regulations. Students also evaluate their own digital privacy, ethics and technology, and the role of bias in a hyperconnected society. Three lecture hours per week. Instructional support fee applies. Gen. Ed. Competencies Met: Critical Thinking, Ethical Dimensions, and Scientific Reasoning and Discovery.

Course Student Learning Outcomes

1. Describe common ecommerce business models and the challenges created by the Internet of Things (IoT). 2 .Explain IT system architectures and computer memory concepts for processing information. 3. Identify common types of malicious attacks and exploits used against IT systems. 4. Describe cybersecurity defense tools, methods, and components. 5. Discuss the applicable laws and policies pertaining to the storage and transmission of data. 6. Construct a computer network and apply cyber defense methods to secure the system. 7. Evaluate personal digital profile using common OSINT tools, analyze the findings, and recommend solutions. 8. Explain the role of human bias and ethics in technology and its effect on information security.
Credits: 3
Program: Computer Information Systems