North Hennepin Community College

CSCI 1050: Computer Security Basics

A. COURSE DESCRIPTION

Credits: 3

Lecture Hours/Week: *.*

Lab Hours/Week: *.*

OJT Hours/Week: *.*

Prerequisites: None

Corequisites: None

MnTC Goals: None

This class examines the issues surrounding computer security in today's highly technological world. The course is designed to provide an overview of security problems: technical issues and the principles associated with databases, networks, administrative controls, privacy, operating systems and programming. The knowledge gained from this course will allow programmers, instructional designers, information technology specialists and managers to better understand a variety of issues surrounding secure computing. It is preferred that students have proficient computer skills.

B. COURSE EFFECTIVE DATES: 01/10/2011 - Present

C. OUTLINE OF MAJOR CONTENT AREAS

1. This course will cover: Firewalls, Trojans, Malware, Federal Regulation, Ethics, and Web Accessibility for ADA compliance, and introductory cryptography.
2. Students should learn about attacks, computer criminals, defense methods and the hardware and software of security.
3. Threats to security topics should include the identification of threats to networks, system protection, wireless security, and an introduction to cryptography.
4. Cryptography introductions should include use of ciphers, their history and the future direction.
5. The management and policy side of security should include disaster planning, viruses, risk analysis, policy development, physical security, the economics of security, and the legal and ethical issues.
6. Personal computing security issues should include wireless computing, Wi-Fi, firewalls for home computers, social networking, Online banking, and ADA accessibility in programming.

D. LEARNING OUTCOMES (General)

1. Define a broad view of Computer Security as information security.
2. Classify the people issues and effects, from a business and technical standpoint, surrounding Computer Security in various organizations.
3. Summarize the types of attacks that can occur.
4. Interpret legal and ethical issues in computer security cases.
5. Examine elementary cryptography.
6. Distinguish the nature of attacks and their economic impact.
7. Analyze cases to determine solutions for secure systems management.
8. Examine web accessibility and ADA issues on the web.
9. Develop a personal computing security plan.

E. Minnesota Transfer Curriculum Goal Area(s) and Competencies

None

F. LEARNER OUTCOMES ASSESSMENT

As noted on course syllabus

G. SPECIAL INFORMATION

None noted