Internet Security Basics

Course Information

Division	Business
Course Number	CMP 114B
Title	Internet Security Basics
Credits	0.5
Developed by	James McBride
Lecture/Lab Ratio	0.5 Lecture/0 Lab
Transfer Status	Non-transferable
Activity Course	No
CIP Code	11.0100
Assessment Mode	Pre/Post Test (30 Questions/30 Points)
Semester Taught	Upon Request
GE Category	None
Separate Lab	No
Awareness Course	No
Intensive Writing Course	No

Prerequisites
None

Educational Value
The primary purpose of this course is to instruct general students on how to protect a PC and Network from external threats.

Description
Designed to provide experience setting up and using: virus scanners, Malware/Spyware/Adware scanners, content filters, spam filters, firewalls, while addressing the topic PC security and identity theft.

Supplies
None
Competencies and Performance Standards

1. Identify the risks associated with using a computer connected to the Internet.

   Learning objectives
   What you will learn as you master the competency:
   a. How Viruses function.
   b. The difference between MalWare/SpyWare/Adware.
   c. What a firewall is.
   d. What SPAM is.
   e. What a Content Filter does and how it works.
   f. What Identity theft is.

   Performance Standards
   Competence will be demonstrated:
   o By installing and using software in each area.
   o By the successful completion of the final exam.

   Criteria - Performance will be satisfactory when:
   o learner identifies the names, purpose, and characteristics, of each topic.
   o learner can successful configure the software packages associated with each topic.

Types of Instruction
Classroom Presentation
On Campus Laboratory

Grading Information
Grading Rationale
Post test 50%
Labs 50%

Grading Scale
A  90-100%
B  80-89%
C  70-79%
D  60-69%
F  0-59%