CTS 155: TECHNICAL SUPPORT FUNCTIONS

COURSE DESCRIPTION:

Prerequisites: None
Corequisites: None

This course introduces a variety of diagnostic and instructional tools that are used to evaluate the performance of technical support technologies. Emphasis is placed on technical support management techniques and support technologies. Upon completion, students should be able to determine the best technologies to support and solve actual technical support problems.

Course Hours per Week: Class, 2. Lab, 2. Semester Hours Credit, 3.

LEARNING OUTCOMES:

Upon completing requirements for this course, the student will be able to:

A. Identify the basic troubleshooting strategies used to diagnose PC issues
   1. Utilize various Windows components, Services and Registry Editors to optimize the PC
   2. Utilize various OS and third party back up utilities to ensure data and registry retention

B. Identify and explain the types of malware threats in today’s PC environment

C. Employ various strategies to safely remove Malware and Spyware.
   1. Employ various methods for preventing infection including system and application updates, anti-virus programs, and other third party scanning and safeguard utilities
   2. Employ various strategies and utilities to safely and anonymously analyze and research malware threats

OUTLINE OF INSTRUCTION:

I. Troubleshooting Strategies
   a. Common strategies
   b. Using and editing the Registry
   c. Services, MSConfig, and Safe Mode
   d. Recovery Console and Disk Utilities
   e. Performance Tools
   f. System Restore
   g. dxdiag

II. Malware Best Practices
   a. Isolating Suspected Malware
   b. Using VMs to Analyze Malware
   c. Using Sandboxes or other Protected Environments
   d. Setting a Baseline
e. Safe Researching Strategies

III. Backing Up the System
   a. Backing Up the System using OS Tools
   b. Backing Up the Registry
   c. Imaging

IV. Protecting the System
   a. System and Application Updates
   b. Installing and Maintaining Anti-Virus Software
   c. Other Third Party AntiVirus Anti-Malware or Lock-down Utilities
   d. The Windows Explorer Phishing Utility
   e. The Windows Firewall

V. Understanding Slow Systems
   a. MultiTasking/ RAM
   b. Virtual Memory
   c. Defragmentation of non SSD drives
   d. ReadyBoost
   e. Setting number of CPUs
   f. Using the Windows 7 Performance Troubleshooter
   g. Disabling Unneeded Services
   h. Memory Leaks

VI. Identifying Malware
   a. Types of Malware
   b. Sandboxes
   c. Malware Analysis
      i. Static
      ii. Dynamic
      iii. MD5 Hashes

VII. Removing Malware
   a. Automated Solutions
   b. Manual Removal Strategies