**Seminar on Computer Use** (Speaker: Mr. Mike Sanderson, IT Analyst, Department of Biomedical, Chemical and Environmental Engineering; Date: June 16; Time: 11:15 – 12:30 PM)

The session opened with an introduction of Mr. Mike Sanderson, the IT analyst for the Department of Biomedical, Chemical and Environmental Engineering (BCEE) in the College of Engineering and Applied Science (CEAS) , given by Debbie Liberi. Mr. Sanderson began his IT career in 1980 being charged with the setup, management and maintenance of a Microdata Sequel mainframe system for an electronics distribution company. In the mid-90s he worked as the Network Administrator for a local insurance company managing all end-user workstations as well as the company’s Microsoft’s (eMail) Exchange Server and Microsoft’s SQL database server. He currently serves as the IT Analyst for the Department of BCEE in CEAS and is currently working on automation techniques for the department using Powershell, as well as recertifying several certifications. Mr. Sanderson earned his undergraduate accounting degree here at UC in the College of Business. He has also earned a number of IT-related certifications such as Cisco’s CCNP (Cisco Certified Network Professional), Microsoft’s Exchange Server and IIS Web Server, CompTIA’s Security+ as well as ISC² CISSP (Certified Information Systems Security Professional).

The purpose of the seminar was to distribute laptop computers and flash drives to the participants of the RET and CEEMS participants during the summer of 2014 and inform the participants of acceptable use of the equipment.

The participants were informed that the laptops run the Windows 7 operating system, rather than the more recent version, Windows 8. Each of the laptops have an installed copy of Office 2013 and McAffee Antivirus software. At this time, the computers are not password protected for use on the University of Cincinnati wireless network, but it was mentioned that the computer can be password protected if it will be used on other networks.

One major concern with the use of the laptops is their infection with viruses. While participants were given flash drives to use with their laptops, they were told not to remove a flash drive from another computer and then plug it into their laptop. Because many viruses launch in the background, as soon as the flash drive is plugged into a computer and recognized, the virus can go to work infecting the computer. Rather than transferring files between computers using flash drives, it was recommended that participants upload their files to an online Wiki page or Google Drive, so that their work is available online for download to any computer.

If a computer does become infected with a virus or have other technical issues, participants were told to contact Mr. Sanderson’s office themselves, or send a message through their group’s coordinators. The session closed with each of the participants attempting to log into the university’s wireless network, using their 6+2 user ID and Password.



**Figure 1: Mr. Mike Sanderson Discussing Usage of the Laptops**