Computer Security

- Computer Security:
  - Password Strength
  - Windows Update
  - Anti-malware/Anti-virus
  - Screen saver
  - Windows Firewall
  - Practice safe computing
- Steps to Secure Computer & Self

Password Strength

- Strong passwords are required to ensure data security
- Weak passwords can be hacked and sensitive data compromised
- Computer security experts recommend the following criteria when creating or changing a password:
  - Password should be at least 10 characters long (the longer the more secure)
  - Password should include at least one uppercase and one lowercase letters
  - Password should include at least one number (i.e. 1, 2, 3, etc.)
  - Password should include at least one symbol – where permissible (i.e. !, @, #, etc.)
  - Password should NOT include names (easier to hack)
  - Password should NOT include dictionary words (easier to hack)
- Demo - https://howsecureismypassword.net/

Windows Update

- The Windows Operating System is massive and includes many security defects
- Crackers (hackers are the good guys) use these back doors and windows to access computers
- Microsoft does a good job fixing these Operating System vulnerabilities as soon as they are discovered
- Windows Update is also used to keep MS Office, Defender and some drivers up-to-date
- One could schedule Windows Update to run (i.e. every Wednesday at 2:00 am) and/or run manually
- Demo

Anti-Malware/Anti-Virus

- Malware stands for Malicious Software
- Malware categories:
  - Viruses (intent is to damage files – i.e. delete, corrupt, etc.)
  - Worms (similar to virus, except it's self replicating – infects other computers)
  - Spyware (Intent is to spy – i.e. gather accounts and passwords information)
  - Adware (Intent is to advertise)
- There are thousands of existing malware on the Internet and new malware is added each day
- It's extremely important that you use a reputable anti-malware/anti-virus software and keep the signature file (signatures of malware) up-to-date
- Microsoft offers a good and free anti-malware/anti-virus package called Defender (of course, there are many reputable anti-malware/anti-virus packages)
- Demo

Windows Screen Saver

- What is a Screen Saver?
  - It's a moving picture or pattern that appears on a computer screen after the computer has been inactive for a configured period of time
- Historically, Screen Saver was developed to save older screens from image burn-in (newer monitors don't that that problem)
- Today, the Screen Saver feature is primarily used to secure a computer by locking it after it's been inactive for a configured period of time:
  - For example, if the Screen Saver is configured to lock a computer after it's been inactive for 5 minutes and the computer user rushes to a meeting, the Screen Saver will kick-in after 5 minutes and lock the computer. Otherwise, the computer will be unlocked for the entire time the user is away, which is a security risk.
- Demo

Windows Firewall

- The job of the firewall is to prevent unauthorized users from accessing computers
- Firewalls can be complex to configure
- However, if one is not sharing any objects (i.e. printer or folder), then one could easily configure the firewall to block all incoming connections
  - NOTE: One could connect to the network and Internet, but others can't connect to the computer
- Demo

Practice Safe Computing

- Most malware come from the Internet (websites and email)
- The Internet is full of poisoned websites (infected with malware)
- Some of the email messages are also infected with malware
- The anti-malware/anti-virus software will protect you from most, but not all malware (not recognized in the signature file)
- It's wise to practice safe computing means:
  - Don't click on every link
  - Don't open emails from unrecognized sources
  - Be careful when providing personal information
  - Be mindful of where you go and what you do!

Steps to Secure Computer & Self

1) Use a strong password
2) Keep the Operating System and Applications up-to-date (Windows Update)
3) Install a reputable anti-malware/anti-virus software and keep it up-to-date (i.e. MS Defender)
4) Enable Screen Saver with password
5) Enable firewall and block all incoming traffic
6) Practice safe computing