Security Recommendations for Desktop Computers

Due to the increase in hacker activity on campus, DSS (in conjunction with other NUIT units) has put together the following recommendations to bolster desktop security:

- All desktop computers should have the free NU version of Norton Anti-virus and should retain the setting that schedules regular updates of virus definitions from the central server.
- When a desktop computer is built, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly, on an ongoing basis. The frequency will be a balance between loss of productivity (while patches are applied) and the need for security. We recommend a two to three week cycle for each machine.
- Whenever possible, security policies should be set at the server level and applied to the desktop machines.
- All Windows desktops (and OSX or later Macintosh desktops) should have an administrator account that is not used as the regular login account. The login for the administrator account should be changed from the default. The password should be a “strong” password, defined as:
  - must be 6-8 characters in length
  - must include punctuation such as ! $ % & * , . ? + - =
  - must start and end with letters
  - must not include the characters # @ ' " ` \ 
  - must be new, not used before
  - passwords expire every 4 months
- The password for the user login should follow the same parameters outlined above.
- The guest account should be disabled.
- New machines with Windows XP or OS X should activate the built in firewall. All users should consider use of a free firewall such as Zone Alarm.
- All machines with Windows 2000 or XP should be checked with the Microsoft Baseline Security analyzer for obvious security holes.
- All compromised machines should be rebuilt from scratch (i.e. erasing the hard drive and starting fresh from installation disks).
- Do not install Microsoft IIS or turn on any of its functions unless absolutely necessary.
- In general, start from a position of security that is most secure (i.e. no shares, no guest access, etc.) and open up services as necessary.

In addition to the above suggestions, DSS recommends a regular backup strategy. It should be noted that even with all the procedures listed above, there is still the possibility of a virus infection or hacker compromise. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss of a machine.

It should be noted that, if a machine is compromised, NUIT security will shut the port off. This will isolate the desktop computer until it can be rebuilt. At that time, the port will be turned back on.

For departments with their own subnets and Administrators, standard filters can be applied at the subnet level. If a department has its own servers, NUIT security personnel can “scan” the servers for vulnerabilities upon request. Finally, these departments would also benefit from having their administrator join the “UNITS” listserv, the security listservs and the specific alert listserv (used when shutting off ports).