

Computer Maintenance, Safety and User Tips

This document is designed to help you be more efficient and provide greater security to the computer, and your account (netID). Following these suggestions should help minimize the number of viruses and defects that infect your machine.

Desktop

The computer Desktop is actually a file that grows and decreases in size, depending on your activities on the computer. Storing files and folders on the Desktop is a dangerous practice. If actual files and folders are stored on the Desktop, and the Desktop file fails, then you stand the chance of losing anything that was stored on the Desktop. Through the use of diagnostic and repair utilities, these items on the Desktop can sometime be recovered and repaired. But, in some cases, the files are lost forever. Therefore, it is important to store actual files and folders within the hard drive (C:/). If you have files and/or folders that you access frequently, you can make Aliases (Mac) or Shortcuts (PC) of the items and place the Aliases/Shortcuts on the Desktop, instead of the actual items. Aliases/Shortcuts are small files (about 15k) that point to the actual item and open it.

- You can create Aliases on a Mac by highlighting the item you wish to alias, then using a keyboard shortcut (Apple Key + L), or go to the "File Menu" and select "Make Alias."
- On a PC, you highlight the item you wish to make a Shortcut of, then right-click with your mouse. A contextual dialog menu will appear. Within the menu select "Create Shortcut."

Password

It is important to keep your netID password to yourself, and not share it with anyone. This netID password identifies you as an authorized user on the NU networks. Having your netID fall into the hands of someone who is malicious, can cause you great trouble with accessing the NU network. Therefore, it is important to keep your password secret.

Your password should consist of at least 6 (six) characters. Within the six characters, your password should contain one of the acceptable symbols, other than numbers and letters. This will keep your password secure, and make it harder for anyone to copy your password and use it with your netID. You should get into the habit of changing your netID password every three months. This will provide more security for your netID and you. NUIT sends out notices when it is time for you to change your password.

To find out more about changing your password, updating your directory listing, activating/deactivating your email while on vacations, mail forwarding, etc., and policies about your netID, please go to the following URL link: <http://snap.it.northwestern.edu>

OS and Virus Protection

The best way to prevent your machine from becoming infected with a virus, worm, Trojan horse, or any other type of malicious code, is to always keep your machines as updated as possible. You should have your machine automatically set to check for OS (Operating System, ie...Windows 2000, WinXP, Mac OS 10.3.X) updates on a regular basis. If your

machine is not set to do it automatically, or you choose not to have this feature turned on, then you should get into a regular schedule of checking for OS updates. You should also run Norton's Live Update on a frequent schedule. Running this utility will update your machine's virus definition file. This file is comprised of a listing of all known virus strings. Keeping this file updated will help reduce the potential for infection.

Macintosh

- To update your Mac OS software, open the System Preferences (found under the Blue Apple Menu).
- Locate the Software Update icon. Double-click on it to open it.
- Select the "Check Now" button to run the Software Update application. The software will contact Apple's OS download site and scan to see if any new updates are available for your machine.
- You can set Software Update to check for new software automatically by selecting the "Check for Updates" feature within the dialog window. Once you have checked this feature, you can determine how often you want the software to go out and check for update. It can be daily, weekly or monthly. Weekly seems to be the best selection.

Windows PC

- To update your Window software, go to the Start Menu and open the Control Panels.
- Locate the Automatic Updates icon within the Control Panels.
- Double-click on the icon to open it. Select the appropriate setting for when you want the software to go out and look for updates, and how you want it to react when it finds new updates.
- Windows allows you to download the software and install it, notifies you when software updates are available for download, and/or downloads and installs the OS updates automatically.

Email

When using email, it is important to closely monitor what is being delivered to your machine. Mail that is not from the NU community, or from someone you know, should be directed to the "Junk" mailbox. Adjusting the "Junk" mailbox properties can be done by accessing the "Settings Menu" from within Eudora. At the left-hand side of the dialog window, locate the "Junk" icon and select it. The dialog window will change at the right, showing you a slide-bar and different features concerning junk mail. You can make adjustments to these settings to filter unwanted and/or unsolicited email to the "Junk" mailbox.

If you receive an email message from someone you don't know, please do not open it or any associated attachments. Hackers frequently distribute malicious code through e-mail attachments. If you are unsure about a specific email, the best practice is to just throw it away...un-opened. Please do not forward any email that you are unsure of. This can cause an epidemic of malicious code coursing through the NU network community...just throw it away.

Web Browser

There are a few things that you can do to help protect yourself while “surfing” the web. They are; clear your history directory frequently, clear your web cache, and delete Cookies. You can do this by opening the Preferences and/or Internet Options (depending on which browser you are using). Within this dialog window, you can clear out your web disk cache, delete your history (web sites you have visited), and/or delete your Cookies.

The last item in the above paragraph is important. You want to get into a regular schedule of performing the above tasks, especially with deleting Cookies. Cookies are little identifiers for specific web sites. These little applets gather information about your web surfing activities, etc., and send this information back to the site that has downloaded a Cookie to your computer. You can shut this feature down within the Preferences/Internet Options, but you will lose the ability to access some sites. It is best to leave this service on within the browser, and getting into the habit of deleting the Cookies on a regular basis. I would recommend deleting your cache and Cookies at least every other week. This will prevent you from unknowingly infecting your machines, and/or the NU network. Not only do Cookies track user information and activities, they are also being used as vehicles by hackers to deliver malicious code to unsuspecting users. Deleting Cookies will also help in reducing the number of “pop-ups” that appear when browsing. In a lot of browser applications, you can turn this feature off, to block all pop-ups. Depending on which browser application you are using, would determine whether you can turn pop-ups off. It is best to have the latest version of the browser application you are using. You can obtain Netscape, Internet Explorer and Safari at their respective manufacturers’ web sites. You can also obtain them from; www.download.com. This web site has the current versions of Freeware, Shareware and Paid software available for download. You can also download other browsers, outside from the three industry standards.

Disk Maintenance

It is important to keep you hard disk up to optimal performance. On a PC, you will want to run Defrag.exe on a regular basis. This will defragment your hard drive and help your machine run smoother. On a Mac, you will want to go to your Utilities Folder, found within the Applications Folder, and open Disk Utilities. Launch this application. This application will analyze you hard drive and accounts for any problems, and give you the option to fix, and/or repair any bad items.

You should get into the habit of running these pieces of software of a regular basis. I would recommend running the software at least once a month. While running these softwares, please make sure no other applications are running. This will impair the application and prevent it from making necessary changes and/or repairs. Plan on time. These applications take some time to run and perform their tasks, because they are performing intensive inspections of your entire hard drive. With hard drives much larger than a few years ago, times to run diagnostic softwares has increased. Plan on doing something else while the diagnostic software does its work.

Any questions, concerns and/or comments, please send them to; Scott Jeffress, s-jeff@northwestern.edu, Ph. 312-503-1026

