BEST PRACTICES FOR COMPUTER SECURITY

This document details how you can secure your personal computer accounts and the data stored on them and contains technical security precautions that you should know and implement. Following some of the suggestions below can affect how your computer interacts with the Internet you should consult with your Internet provider before making changes to avoid disrupting your Internet connection.

ACTIONS TO PROTECT YOUR COMPUTER

- Use security software
- Practice the principle of least privilege (PoLP)
- Maintain current software and updates
- Avoid threats to your computer
- Never share passwords or passphrases
- Do not click random links
- Beware of unknown email and attachments
- Don't download unknown software off the Internet
- Don't propagate hoaxes or chain mail
- Log out/lock your computer
- Shut down lab/test computers
- Remove unnecessary programs
- Restrict remote access
- Frequently back up important files
- Treat sensitive data carefully
- Remove data securely
- Deploy encryption when possible
- Securing your home network

USE SECURITY SOFTWARE

The most important thing you can do to keep your computer safe is to install and maintain security software, which protects your computer from viruses and spyware. Such security programs perform two general functions: scanning for and removing viruses and spyware in files on disks, and monitoring the operation of your computer for virus-like activity (either known actions of specific viruses or general suspicious activity). Most software can perform both of these tasks.
Install an antivirus application, and keep your virus pattern files up to date, In general, it's not a good idea to have more than one antivirus program installed on your computer. Each program may interpret the actions of the other as viral, therefore giving you false warnings about virus-related activities.

PRACTICE THE PRINCIPLE OF LEAST PRIVILEGE (PoLP)

Practice the principle of least privilege. Do not enable administrative privileges until needed (i.e., do not log into a computer with administrative rights unless you must do so to perform specific tasks).

Running your computer as an administrator (or as a Power User in Windows) leaves your computer vulnerable to security risks and exploits. Simply visiting an unfamiliar Internet site with these high-privilege accounts can cause extreme damage to your computer, such as reformatting your hard drive, deleting all your files, and creating a new user account with administrative access. When you do need to perform tasks as an administrator, always follow secure procedures.

MAINTAIN CURRENT SOFTWARE AND UPDATES

Use a secure, supported operating system and keep your software updated by applying the latest service packs and patches. For Windows, you can schedule *Automatic Updates* to automatically download and install available updates.

AVOID THREATS TO YOUR COMPUTER

Never share passwords or passphrases: Pick strong passwords and passphrases, and keep them private. Never share your passwords or passphrases, even with friends, family, or computer support personnel.

Do not click random links: Do not click any link that you can't verify. To avoid viruses spread via email or instant messaging (IM), think before you click; if you receive a message out of the blue, with nothing more than a link and/or general text, do not click it; delete it.

Beware of email or attachments from unknown people, or with a strange subject line.

Do not download unfamiliar software off the Internet: Some programs appear to have useful and legitimate functions. However, most of this software is (or contains) spyware, which will damage your operating system installation, waste resources, generate pop-up ads, and report your personal information back to the company that provides the software. Obtain public-domain software from reputable sources, and then check the newly downloaded software thoroughly, using reputable virus detection software on a locked disk, for signs of infection before copying it to a hard disk.

Log out of or lock your computer when stepping away, even for a moment: Forgetting to log out poses a security risk with any computer that is accessible to other people (including computers in public facilities, offices, and shared housing), because it leaves your account open to abuse. Someone could sit down at that computer and continue working from your account, doing damage to your files, retrieving personal information, or using your account to perform malicious actions. To avoid misuse by others, remember to log out of or lock your computer whenever you leave it.

Remove unnecessary programs from your computer.

Restrict remote access: It is recommended that you disable file and print sharing. In rare exceptions when you may need to share a resource with others, you should format your drive using NTFS, and correctly set the file and directory permissions. With Windows 2000 and XP, new folders are created by default with access granted to the "everyone" group. If you do have file sharing enabled on your computer, be careful to set permissions correctly when creating new folders so you don't inadvertently leave them open to everyone on the network.

Frequently back up important documents and files: This protects your data in the event of an operating system crash, hardware failure, or virus attack. Make sure to save files in multiple places using two different forms of media (e.g., USB flash drive, or CD-R).

Treat sensitive data very carefully: For example, when creating files, avoid keying the files to Social Security numbers, and don't gather any more information on people than is absolutely necessary.

Remove data securely: Remove files or data you no longer need to prevent unauthorized access to them. Merely deleting sensitive material is not sufficient, as it does not actually remove the data from your system.

Deploy encryption wherever it is available.