

Safe Computing – Best practices - An individual's responsibility

If you use a computer on a daily basis you will need to perform some common tasks to keep it running well. Keeping it well tuned will reward you with daily reliability and solid performance. There are several areas that need attention as follows:

➤ Personal Security

Check your antivirus for proper operation and updates - Antivirus protection should be updated and checked weekly. A weekly scan for viruses should be scheduled, if not, run a manual scan weekly.

Don't give out your work email address online unless it is for official business - The best way to reduce junk mail is by not giving out your address unless it is necessary in the performance of your job duties. Do not participate in joke/junk mail circles. Your address gets forwarded on to everyone else who ever reads it in the future.

Don't check your personal email while at work - Doing so subjects your office computers to unnecessary risk. If you must check personal email at work please get authorization from your supervisor.

Don't participate in P2P file sharing – Peer to Peer systems like Kazaa, Morpheus, etc, allow you to download music, movies, and software. These files not only have a high rate of being infected with viruses but also put your office and yourself at risk of prosecution for copyright infringement.

Avoid game and screensavers sites – Many game sites will require you to install an add-on to internet explorer. Some of these add-ons can be harmful to your computer and others can take your internet over completely. Screen savers are programs. Screensaver websites are a known source of viruses and malware. As well, poorly written screen savers can cause performance problems with your computer. They may not unload from memory fully or can cause memory faults because they are trying to use memory already being used by windows or other programs.

Turn off the preview pane (reading pane) in your email client – With the preview pane on, you can't select an email to delete it without opening it in the viewer. Turning off this preview will allow you to select and delete without ever opening the mail. Disable for inbox, junk, and deleted items.

Report any suspicious activity or unexpected computer events to your supervisor – If your antivirus reports a virus or your homepage suddenly changes you should report this to your supervisor. Odd behavior can be your warning that something is about to go wrong. It may be that your computer and or data have been compromised and this should be investigated further.

Store highly sensitive data in encrypted form– There are many 3rd party programs available to encrypt data so you can store it in scrambled form. AxCrypt and Truecrypt are a few free ones. Extremely sensitive data should be deleted by a shredder program. They overwrite the area of the drive where the file was stored multiple times. Spybot S&D (has a file shredder built in) and AbsoluteShield are both free. Never expect (or even ask) to retrieve files that have been shredded. CAUTION: If you shred important operating system files you will render your computer inoperable.

Windows Updates – Windows updates comes in 2 forms, Automatic and Manual and 2 flavors, Windows updates and Microsoft Updates. Most users will install automatic updates routinely

because they get reminded by the balloon popup every time they log on. Users should periodically perform a manual update by going to the windows update site. Click on tools in Internet Explorer menu and select "Windows Update". The first time there you should sign up for "Microsoft Updates" This will allow updates for other Microsoft products (Word, Excel, etc) to be installed as well. After signing up for "Microsoft updates", you should repeatedly come back to this site until it shows 0 (zero) critical updates available. Manual updating should be done every 6 months at the longest. Vista users will have to use the integrated windows update tool in the programs menu.

➤ Common Maintenance Tasks

Backup your data – Hard drive failure can occur at any time and retrieval of critical documents can cost thousands of dollars. CD and DVD backup are available to most computer users. Flash drives (USB thumb drives) are an alternative low cost solution and there are plenty of free programs to assist you with the backup process. Critical information subject to the privacy act should be encrypted then the encrypted file should be backed up to external media. Some USB flash media is available with built in encryption and would be preferred for persons handling sensitive data. Only remove backup media from the office with the permission of your supervisor. Always ground out any static discharge from yourself before inserting a flash drive into a USB port.

Tape Backup – If you have a tape drive you should also have a cleaning tape for it. Insert the cleaning tape before every weekly (system) backup to insure the tape drive heads stay clean. Cleaning tapes are available thru LGC or your office supply vendor. Replace backup tapes annually to insure reliability. If you are still using Travan tapes please consider upgrading. The lower cost DAT tapes will pay for the upgrade in a couple of years and they are 3 to 4 times faster at backing up data.

Disk Cleanup – Temporary internet files and other temporary files build up in your computer. Disk Cleanup removes old junk files from your computer. XP users should not compress old files. This can make them harder to recover and can significantly slow down your computers operation.

Disk Defragmenter (hard drives and removable media) – File fragmentation is a normal occurrence in most computers. It happens when you use them. If a hard drive becomes too fragmented it will degrade the computers performance. Periodically run disk defragmenter on all drives including flash drives to keep your computer running smooth.

Ventilation – Proper case ventilation is critical for the life of your computer. Dusty environments require more frequent cleaning of the fans inside the case. Do not block off air intake grills.

Temperature - Computers are fairly sensitive to temperature extremes. Proper operating temperature is about 70 deg F. If your office is not heated at night or the temperature is reduced then you should let your computer warm up for awhile before you turn it on. If the temperature falls below 50 degrees or raises above 85 degrees you should shutdown your computer or serious damage could result.

Remove unused/unwanted software – Add remove programs (Programs and Features for Vista users) in the control panel is the proper place to remove unwanted software. If unsure of what software is safe to remove, consult your supervisor. Printer software (for disconnected printers), Google toolbar, Ask toolbar, Yahoo toolbar, Google desktop search, coupon shopper, etc, are all safe to remove.

Set a schedule - Schedule these maintenance tasks on an interval that is frequent enough to insure they get accomplished (not forgotten) but not so frequent that they interfere with office operations. Monthly is sufficient for most tasks in the average office. Backup personal data daily or weekly.

➤ Liabilities

Administrative Rights and Passwords – All computers need a password for access to it. Most computer users have administrative rights to the computer. If you visit a website, they (the site owners) can learn your username from your computer easily. If you haven't set a password yet, gaining control of your computer is much easier.

Free is seldom truly free – These days information is a valuable commodity. They want your info.... If giving you a piece of poorly written software is all it takes to get your email address then it's a small cost to them. Always read their privacy policy and EULA (End User License Agreement). Check out any software you download thru several channels of investigation.

Trojans, Viruses, and Worms – Can attack your computer and do serious damage, the worst of which is not noticeable. Stealth viruses run in the background, giving the use of your computer to others. This allows the creators of the virus to use your computer to do malicious deeds to others while making it trace back to you.

Malware - is software designed to infiltrate or damage a computer system without the owner's informed consent.

Downloader's – Downloader's and Droppers continually download and re-infect a computer with many viruses, malware, and Trojans.

Shares – Shared files, folders, and printers on a computer network is the weakest link in office security. If you must share a folder then share as read only. Writable shares can have their contents deleted, modified, or infected if not properly secured. Properly securing a share is not a task for the average computer user. If you must share, please read up on proper methods of authentication controlled access first. Network enabled printers have eliminated the need to share a printer from a computer because network users can access it directly from their workstation or server.

Media – Recordable CD-RW and DVD-RW media have a limited life expectancy. These disks are good for about 500 writes and then they should be disposed of. When stored in perfect conditions write once and rewritable media are only expected to last 5 to 10 years. USB Flash drives have a limited lifespan as well. While they may have a MTBF (Mean Time between Failures) of over a million hours, they are only designed to handle so many writes and erases before they expire.

Reporting responsibilities – If individual office personnel do not report virus activity they put the whole office at risk. It is everyone's responsibility to insure the security and integrity of personal data. The one place that you don't want to learn about your security breach is on the news. Government and Corporate offices are incorporating network monitoring systems to track data transfers and internet usage.

Office Policy – A good office policy states boundaries for proper use of office computers and internet. It can help to protect your data's security and reduce costly downtime and repairs. Sample digital security and internet use policies are available at Http://Greysville.com/LGC/Sample_policies.htm.

➤ Additional Notes

Free antivirus programs rarely protect you from Spyware – Buy one that does. Most free antivirus programs are not licensed for use on government or commercial business computers.

Never install more than one antivirus program on your computer – It will break your computer.

Avoid falling victim to scare tactics – Analyze everything.... Scare tactics come from many sources, Email warnings, website pop-up ads, etc, warning you that your computer is infected. And they are getting more frequent. They are designed to convince you to take some action that will ultimately be harmful to your computer. The safest way to close a popup webpage or rogue program is to hit CTRL-ALT-DEL and click on Task Manager. Select the internet explorer instance or program that you think is the proper one and click on end task.

Get a second opinion - Freestanding programs are available that can provide you with a second opinion of your virus/malware status. Stinger (from McAfee) is a good standalone antivirus but it only detects the most common viruses. Malwarebytes is an excellent choice for standalone malware removal. Online scanning for malicious software can be done at several antivirus vendor sites.

New or unknown viruses and malware – All malware spends some time as an unknown. There is always some time lag between when a virus or malware gets created and when you are protected from it. Someone has to get it. It has to be identified as a virus. Antivirus vendors have to update their detection schemes to detect it and you have to download the update. This can take weeks during which time you are vulnerable to the new attack. The only 100% protection for a computer is not to have it connected to any network or internet at all. Even then, CD's or flash drives that are infected can be inserted infecting even the invulnerable.

Automation instills complacency – Automation is the way of the future. But it makes us lazy. If you schedule automatic tasks make sure you confirm their proper operation periodically.

Fire Hazards – Leaving equipment running in unmanned offices is a fire hazard. Mission critical equipment that is left on should be monitored by a fire/smoke detector that will provide an outside alarm if the building is unmanned at night.

Sleeping your computer - All computers should be shut off at night unless maintenance events are scheduled. Sleeping or putting your computer into standby is an acceptable alternative to shutting down every night. It allows for a quick wake-up but stops all the moving parts when asleep. Do not turn off your battery backup if you want to sleep your computer at night as it keeps your computer's memory active during the sleeping process. A power loss at night will reset your computer and can cause data corruption or loss so always save any open documents first. Note: If you decide to sleep your computer, please realize that it uses more power than shutting down fully and turning off the battery backup. It also increases fire risks as well as the storm damage potential because you still have equipment running. You should periodically shutdown fully to allow the computer a fresh boot.