

# COMPUTER HELP!

## NEWSLETTER 2010

By Ed Siemion, Computer Consultant

Greetings!

Thank you for requesting services. In this year's newsletter, focus is security and protecting equipment.

- **Securing from Malicious Software**
- **Online Buying and Social Networking**
- **Securing Information**
- **Protecting Physical Condition of Computers**

Does it make sense to setup an entertainment system, coffee table and sofa in a bank vault?

This is what many attempt with a single computer system...secure home or business financial then use for music, photos, video, social networking and more.

To reduce problems, work to keep computer limited to a specific set of tasks and those who use it.



**(206) 235-7911**  
**Ed Siemion, BS, MS**  
*On-Site & Remote Desktop Support*  
*Home & Business: [www.apexinformationservices.com](http://www.apexinformationservices.com)*

## Securing from Malicious Software

As a result of 9 years of global use, the Windows XP operating system has been determined to be the most “hacked” computer operating system in history.

Instead of XP, use the “latest” operating system from Apple or Microsoft.

On release of Microsoft’s Windows 7, nearly 100% of existing threats to a Windows computer were made obsolete.

When a computer is connected to the Internet or accepts files from external storage, that computer is at risk.

*In 2007, sensitive information systems managed by our military, had been “hacked” into, information stolen.*

*A set of USB jump drives had been slipped into offices. These jump drives released malicious software of which ran full course, creating a back door resulting in “Terabytes” of information downloaded by the creating end.*

*Afterward, the USB jump drive (or thumb drive) was then banned from use on many US military computers (60 minutes, November 2009).*

Pathways of Malicious Software:

- 1.) External Storage: USB jump drive, CD, DVD, hard drive, floppy, camera card, etc..
- 2.) Communication Interface: Internet connectivity, dial-up modem, other.

Of these two pathways, the Internet is focal. Visiting a website or opening an E-mail message.

When visiting a website, files are downloaded to the computer automatically.

The makers of malicious software work in a clandestine environment one step ahead of security software. Security software such as Norton, McAfee and AVG, SpyBot and others help although fail and perturb operating performance at a PC

*Installing security applications at a computer from Apple is unheard of.*

*With both operating systems from Apple and Microsoft, the privileges assigned to a user logged onto that computer dictate much of the security.*



**(206) 235-7911**  
**Ed Siemion, BS, MS**  
On-Site & Remote Desktop Support  
Home & Business: [www.apexinformationservices.com](http://www.apexinformationservices.com)

It is more secure for a user to login at a home or business computer where after doing so, there is no way such user can immediately install software.

A user is logged on under a "Restricted", "Limited" or "Standard" account with Microsoft-Windows or with Apple-Mac a "Standard" or "Managed with Parental Controls" as opposed to an "Administrative" user account.

## Online Buying and Social Networking

A confirmation E-mail message is received from what appears to be from a reputable online retailer such as Amazon.com yet in reality is not from Amazon.com!

A defense is to use an E-mail address of which is only used for online buying.

This allows your primary E-mail address to never receive a confirmation E-mail message. If it does, you know for sure it is a spam-scam.

All websites which become "common place" are exploited by makers of malicious software.

Common Place Websites:

**Financial Institutions:** Bank of America, Chase, Wells Fargo, etc..

**Social Networking:** FaceBook, Twitter

**Online Retailers:** Amazon.com, Buy.com, NewEgg.com, etc..

Am astounded how many people have learned to trust [www.facebook.com](http://www.facebook.com) with personal information regardless of privacy settings at this website.

Not only has a pathway to personal information and activities been opened, but it also opens opportunity for makers of malicious software to hack into your computer via spam-scam.

*An E-mail message from "FaceBook" will arrive,....Are these safe or not?*

*Recommend to never open any E-mail message from an online retailer, social networking site or any other "common place" website at a computer running mission critical applications.*

When performing routine and daily online buying or social networking, it is more secure to use a web mail account (Gmail, Hotmail, Yahoo), and use a computer of which is locked down (restricted user account) and not used for anything else.---*Avoid using a Windows XP computer.* For tight security, try to only use a computer from Apple



(206) 235-7911  
**Ed Siemion, BS, MS**  
On-Site & Remote Desktop Support  
Home & Business: [www.apexinformationservices.com](http://www.apexinformationservices.com)

running OS X and avoid software supporting browsing Internet and downloading E-mail of which is the most highly distributed such as Microsoft Internet Explorer and Microsoft Outlook, respectively. In the future, the coin may be tossed with Apple less secure than Microsoft having issues with malicious software. In 2010, this is not the case as the “hacked” Windows XP operating system is shipped with many new computers.

## Securing Information

To secure information at a computer, the information is to be preserved and kept private.

To preserve, it is best to have multiple copies. This means “backing up.”

Who should not have access to this information?

How long should it be kept private?

Should the information best be destroyed at some point?

What level of inconvenience or costs to keep information private can be tolerated?

The more information one collects and wishes to secure, the greater will be the cost to do so. Demand can require more hard disk space, backup drives, backup tapes, passwords and other.

A common scenario with many folks are photos and how to secure them. Hard copies of photos look good and provide another storage location other than at a computer.

Again, create multiple copies in a suitable form.

Some online services are available such as from Apple called “MobileMe” which stores photos, contact information, calendar information accessible from an iPhone or any computer at a fee of about \$100/year.

Some methods are free yet can require fancy steps as follows:

*Create a free Gmail account with Google; Compress accounting files from Quicken or QuickBooks into a password protected file; Attach file to E-mail message; Finally send to Gmail account or a couple other online free web mail accounts (Hotmail, Yahoo). Chances for losing it are low. Is password protected where if mail account is hacked, the hacker will likely not bother attempting to crack such password to an already obscure message among thousands.*



**(206) 235-7911**  
**Ed Siemion, BS, MS**  
**On-Site & Remote Desktop Support**  
**Home & Business: [www.apexinformationservices.com](http://www.apexinformationservices.com)**

*Acceptable security for some, yet not for others who desire tighter security/privacy.*

For a business managing all types of computer files (photos, documents, spreadsheet, database)--- standard equipment is a tape backup system, coupled with a redundant system for backing up to hard disk drive in some manner.

With tapes, many copies can be retained in a small package, stored in a vault, and stored off-site.

What does one do in a Katrina hurricane or Haiti earthquake? Where is the backup system now?

*During the 1906 earthquake in San Francisco, fire ravaged everything, including bank vaults which many could not protect deposits. The founder of "The Bank of Italy", Amadeo Giannini physically moved all deposits out of his bank and away as the disaster transpired---As almost none of the deposits at other banks survived, only this bank did enough to become the most dominate bank then, now Bank of America (Wikipedia, 2010).*

Keeping information stored in separate physical locations is important yet may not be depending on what is at stake.

Keeping information private can be tough when an extended time frame is considered.

Is one day of privacy sufficient, 1 year, 50 years or more?

The makers of the Egyptian pyramids desired eternity and built massive stone structures to house that to be preserved---have been intruded upon over centuries. No one wishes to have their banking information revealed yet such information can be compromised solely due to an issue with the retailing or banking industry.

One solution can be to change account number or passwords routinely; yet now banking system can become intolerable to use. Compromises for practical use must be made. Where compromises are made, a hacker digs in.

Privacy can be compromised with an audio/video signal. What recording devices are present these days and where? The "high definition" associated with recording devices is now better than ever.

A password can be revealed to a camera recording hand motions at a keyboard, lip reading, etc. where any action associated with allowing entry/access is of interest to a hacker. Privacy at a computer in most cases depends on a single password or a combination of usernames/passwords.



**(206) 235-7911**  
**Ed Siemion, BS, MS**  
On-Site & Remote Desktop Support  
Home & Business: [www.apexinformationservices.com](http://www.apexinformationservices.com)

One of the most secure logon methods I have seen at a computer used a password which changed every 30 seconds or less. The current password is synchronized every 30 seconds with a small hand held device the size of one's finger where the password is shown to the owner of that device.

## **Protecting Physical Condition of Computers**

It is important to understand how environmental stress plays a role when working to protect condition of equipment.

A power outage can lead to damaged equipment, although sometimes it is not the fact that the power failed as it is when the power is restored at the wrong time or in wrong manner. When bracing for a power outage, it is best to power down sensitive equipment first and unplug before the event occurs. Avoid plugging sensitive equipment back in until power is restored.

Having backup power can help.

A laptop is often one of the best systems to have with respect to power outages as a battery is built in. With desktop computers and networking equipment, a separate source of power such as from independent battery or battery system is required to keep going and to better protect equipment.

For most situations in a home or office, a loss of power is often only a fraction of a second, or few minutes and rarely more than a couple hours. This is enough to crash a desktop computer and connection to the Internet. A battery arrangement can secure operations and protect equipment.

Most computers in a home or office are not entirely solid state. The internal hard drive, containing valued information such as Word documents and photos is typically spinning at 5,000 to 7,200 rotations per minute. The internal cooling fans also comprise mechanical parts subject to failure. These moving parts often are associated with computer failures over time. When power fails and a hard disk drive is spinning at top speed, attempting to save a file during such an event can lead to disk failure. A hard disk drive can fail immediately if bumped, is subjected to excessive heat, cold, moisture, or pressure.

A laptop is the most insecure type of computer to save information and the most difficult to protect from physical failure...is more subject to environmental extremes as opposed to a desktop computer situated in one location. Yet again, all laptops have batteries built-in to protect against power failures.



**(206) 235-7911**  
**Ed Siemion, BS, MS**  
**On-Site & Remote Desktop Support**  
**Home & Business: [www.apexinformationservices.com](http://www.apexinformationservices.com)**

The number one threat to all forms of electronic equipment is heat. Other environmental stresses are important and obvious (shock, liquids), yet stress due to heat is more overlooked.

New computers for home and office have internal power supplies operating somewhere between 250 and 900 watts. More common with a typical desktop PC is a 400 Watt power supply. The more accessories plugged into a computer---the more heat will be produced inside the computer case. Overloading a Windows or Apple computer can lead to heat build-up and premature failure---this means having too many USB devices, add-on adapter cards and, hard drives and anything else “plugged in.”

With special attention to cooling and not overloading the power supply, a “loaded” system can run without problems.

The following lists problems/solutions associated with heat and overloading.

- 1.) Laptop left powered on, not running on standby, is resting on sofa or clothing item.

This can lead to laptop failure. Cooling vents are blocked, internal circuits may overheat and short circuit (burn out)---can also cause a fire. Never leave a laptop powered on crowded by clothing and paper.

- 2.) Keep equipment out of direct sunlight. Avoid leaving in car overnight during cold weather or extended hours during hot days of Summer.
- 3.) Keep computer in dust free environment. Dust will clog cooling fans and air-spaces needed to provide proper air flow and heat transfer away from the processor, memory, video adapter, hard drives, power supply and other internal parts. If in dusty environment, use air-flow filters and clean computer case as needed. Clean computer using blown dry air (leaf blower, vacuum in reverse). Avoid using compressed air from can as these may super-cool parts, create moisture and is not effective for heavy dirt/dust.

Some computers are “liquid cooled” and are not always a good choice. Have seen these systems leak and burn out as a result of coolant loss, failed pump and clogged heat exchanger. The less moving parts to achieve cooling, the better it is to manage and the longer it will last.

- 4.) Avoid operating computer in closed cabinet or hutch. Many newer desk systems provide a cooling fan or an existing desk system can be modified to improve cooling.



**(206) 235-7911**  
**Ed Siemion, BS, MS**  
**On-Site & Remote Desktop Support**  
**Home & Business: [www.apexinformationservices.com](http://www.apexinformationservices.com)**

- 5.) Avoid overloading a 110-VAC circuit in home or office. Often, a home office will have only one circuit routed to all wall receptacles in room...laser printer, scanner, 3 computers, space heater in next room, bright lights. This is overloaded. A tripped circuit breaker is not desired, nor is a fire or failed equipment as a result of overloading. If more equipment is needed, have one or two more dedicated circuits routed to room or split equipment into other rooms using a another circuit.
- 6.) If much equipment in room, recommend air-conditioning during Summer months to cool as needed.
- 7.) If using computer for home entertainment system such as Windows 7 Media Center leaving powered on 24/7, multiple TV tuners for recording programming and other tasks such as gaming---Upgrade cooling fans inside PC. Importantly, keep in location of which itself has adequate air circulation and preferably does not exceed temperatures of 80 deg F or go lower than 50 deg F.

The less plugged into a computer, the less connections, the less moving parts, the less can go wrong.

Hope this has been informative and have a great 2010!



**(206) 235-7911**  
**Ed Siemion, BS, MS**  
**On-Site & Remote Desktop Support**  
**Home & Business: [www.apexinformationservices.com](http://www.apexinformationservices.com)**