

SAFE COMPUTING TIPS

1. Install or Update Your Antivirus and Antispyware Software:

Antivirus and antispyware software are designed to prevent and detect malicious software programs on your computer. In order to keep your computer and your identity safe all computers connected to the internet for any length of time should have both of these products installed at all times.

2. Run a Full Scan With Both Your Anti-virus and Anti-spyware Software:

Full scans with your antivirus and antispyware software can help to catch the most recent viruses and spyware that may have been installed on your computer without your knowledge. Full scans of your entire PC should be run at least daily.

3. Ensure Your Operating System is Up to Date:

Computer operating systems need to be updated to stay current with any security patches released by the maker of your operating system. In most cases people are running a Microsoft operating system that can be checked by visiting <http://update.microsoft.com>. Microsoft usually releases new updates once a month, but may do so more often when an update is extremely critical.

4. Keep Your Software Up to Date:

In addition to keeping your operating system up to date you should also look for updates for the software installed on your PC. This includes software such as Adobe products, Java, Firefox, and Apple iTunes. Software such as this can be vulnerable to hacker attacks and may lead to the compromise of your system if it isn't updated.

5. Keep Your Firewall Turned On:

A firewall helps protect your computer from hackers who may try to gain access to your computer and the information it contains. Software firewalls are available to protect single computers and are even included with many updated copies of Microsoft Windows.

6. Change Your Passwords to Banking, Email and Ecommerce Sites Regularly:

Passwords are the keys to your internet kingdom. Changing your passwords regularly will help ensure the security of all your online accounts as well as the information and the money they give you access to. When changing your password be sure to use strong passwords. Strong passwords use eight or more characters with random letters, numbers, and symbols. In addition, you should never use the same password on multiple sites. If one site is compromised your other accounts could possibly be accessed by thieves.

7. Be Careful What You Download:

You should never open email attachments or click on links in emails from people you don't know. You should also be wary of forwarded attachments and links from people you do know. This is because many email attachments and links can circumvent even the best anti-virus software. Additionally, you should be wary of downloads from trusted and un-trusted sites that seem new or suspicious. If the site has been poisoned or compromised by hackers you could unknowingly be installing a virus or spyware. If you question whether a download is necessary to access a site you can always contact the company for further information.

8. If Possible Have a PC Dedicated Only to Online Banking Activities.

Fraudsters and scam artists have learned that many small and medium sized businesses use online banking products due to their convenience. What they have also learned is that these same businesses often do not take the time to adequately protect the PCs as outlined in these tips, nor do they regularly review their accounts for fraudulent activity. Using this knowledge fraudsters and scam artists are now actively targeting small and medium sized businesses using phishing attacks, email attachments, and web sites designed to take advantage of OS and software flaws. Small and medium sized businesses can protect themselves even further by not using the PC they use for Online Banking for regular web surfing or checking email. These activities can increase a business's risk of unknowingly coming into contact with malicious sites and software.