

Due to an increased risk from viruses and spyware we would like to remind everyone how to check and protect your computer for and from malicious infections.

**1. Install or Update Your Antivirus and Antispyware Software:**

Antivirus and antispyware software are designed to prevent and detect malicious software programs on computer. In order to keep your computer safe 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 Antivirus and AntiSpyware Software:**

Full scans with your antivirus and antispyware software will catch the most recent known viruses and spyware that may have been installed on your computer without your knowledge while using the internet. Going forward you should regularly scan your computer to ensure there are not any infections that you were unaware of.

**3. Ensure Your Operating System is Up to Date:**

Computer operating systems need to be updated to stay current with any security patches found by the maker of your operating system. In most cases, people run a Microsoft operating system which can be checked by visiting <http://update.microsoft.com>.

**4. 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.

**5. 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 numbers and symbols included.

**6. 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 untrusted 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 from a site you can always contact the company for further information.

As always, please be sure to be aware and alert while using the internet. Also, stay tuned to our website for a new education center related to identity theft prevention that is coming soon.