



Keeping Your IT System Protected

Malicious software (“malware”) is one of the most troubling security issues for small businesses. Not long ago, all you needed to keep your businesses IT system safe was to have up to date anti-virus software and a properly configured firewall and you were in pretty good shape. Today, haphazard security means you are risking the function of your IT system and your company's valuable data.

Viruses have long been a challenge. Viruses attempt to replicate themselves for the purpose of affecting the greatest number of PC's (often worldwide), sometimes doing damage in the process. Over time, through a combination of awareness, education and technology we have learned how to protect our IT systems from the vast majority of viruses by having an up to date anti-virus program running at all times. Even so, the threat of viruses still exists with estimated annual damage cost running into the tens of billions of dollars.

So what can you do to protect your IT systems? Here are some important basics which can get you on the right track.

- 1) Be a defensive driver! The vast majority of malware is acquired by visiting unscrupulous websites, opening malicious emails or downloading shareware or freeware from the Internet. In particular downloading music, search toolbars, free desktop icons, free software promising to fix your PC are all good examples of malicious software. Clients often have the idea that their firewall or antivirus program will automatically protect them no matter what they do. This is not true.
- 2) Install and maintain a leading malware prevention program on your workstations. Vipre Enterprise Premium by Sunbelt Software is a relatively new one that I currently recommend. Scan your systems nightly and make sure that threat notification is turned on so you know when a problem occurs.
- 3) Consider using a proxy server (hosted or owned) or security appliance to filter out malicious content before it enters your network. Don't wait until the enemy is inside your fortress!
- 3) Instead of using Microsoft Internet Explorer as your internet browser, consider using Mozilla Firefox. Even though IE8 is more secure than ever, it is unnecessarily complex and cumbersome. I continue to recommend Firefox which can be downloaded from Mozilla.org at no cost.
- 4) Make sure that you are regularly applying updates to your 3rd party applications such as Adobe Reader, Adobe Flash, your internet browser and finally to your operating system. Ignoring this task is one of the most common mistakes people make!
- 5) Make sure that you are regularly backing up your important data.