

## **Are You Making These Security Mistakes When Surfing The Web?**

Does your computer ever run slow, act funny, or crash unexpectedly? Do you get a ton of pop-up ads, even when you are not actively surfing the web? Has your browser been “hijacked” and replaced with another unknown browser? If so, your computer is infected with malicious spyware and viruses that can alter your computer, steal your confidential information, and disable the use of your PC, leaving you without a computer for hours or days while you get it fixed.

And what’s worse –most times once your computer has been hit by these threats, it has to be completely wiped in order to fix it. Unless you have a backup image (a snapshot of everything on the PC, exactly as it is), it will never quite be the same again. You may lose software programs that you downloaded, but don’t have the disk for, your icons won’t be where you remember them, and “little” things like your default printer could be all screwed up. It can be a nightmare.

One big misconception many computer users have about spyware and viruses is that these programs somehow invaded their computer through no action or fault of their own – in most cases, this is simply not true.

Malware, spyware, and viruses are usually a result of some action taken by the user (you or an employee that uses your computer). Remember, cyber criminals are *incredibly clever* and gain access to your computer via some of the most innocent and common activities you are performing; that is why it SEEMS as though it is your computer’s fault when in reality, YOU are unknowingly giving these hackers and auto-loading devastating programs free access to your computer.

Deadly programs to avoid are free “enhanced” web browsers, screen savers, and just about any “cute” programs you come across that are free to download. Always read the terms and conditions before downloading ANY program to look for clauses that allow them (the software vendor) to install spyware programs on your computer.

Unfortunately, installing programs is not the only way a hacker or malware program can access your computer. If you do not have the most up-to-date security patches and virus definitions installed on your computer, hackers can access your PC through a banner ad on the web that you accidentally clicked on or through an e-mail attachment that you opened.

Hackers have also figured out ways to install malicious programs on your computer via your IE web browser, EVEN IF YOU DIDN’T CLICK ON ANYTHING OR DOWNLOAD A PROGRAM. Microsoft is constantly providing “patches” to their operating system software, and all it takes is one missed update to leave you completely vulnerable.

That’s why it’s so important to have someone in charge of updating your computers and server DAILY. An innocent web search by an employee can end up bringing on a host of viruses, hacker invasions, or other evil attacks that end up costing you hundreds or thousands in lost wages and repair costs.

So remember to surf cautiously but also to check with your IT service provider to see what else you can be doing to protect your network and make sure you’re getting the latest patches and updates automatically.