



Seltek Tech Tips April 2011



For more information about any of these topics, contact the Seltek Help Desk at (804) 360-4490 x7 or [e-mail us](#).

Insight: Internet Explorer 9

Recently, Microsoft has released the Beta version of Internet Explorer 9. It is advertised to include faster browsing, more security, and a sleeker, different look. Some new features include:

- * Reopen accidentally closed tabs.
- * Websites can be pinned to the taskbar in Windows 7.
- * More security, such as highlighting known deceptive website addresses in the address bar.

Windows XP Users will not be able to upgrade to Internet Explorer 9 -- you'll need Vista or Windows 7. However, Internet Explorer 9 is still in Beta, meaning it is not a finished product. There may still be bugs, security flaws, and there have been reported compatibility issues with some webpages being unusable with this new release. Seltek recommends staying with Internet Explorer 8 for now.

Symptoms of a Virus or Malware Infection

By Kara Mueller, Primary Help Desk Analyst

There have been a high number of computers infected with viruses and malware in the past month. Here are some symptoms of a possible virus or malware infection. If you are experiencing any of these and suspect your PC is infected, contact the Seltek helpdesk at 360-4490 or [click here](#).

Unusually Slow PC

Many types of malware will make your PC seem much slower than normal. You might notice a slowdown when:

- Starting up the computer
- Checking e-mail
- Going to the internet
- Performing normal tasks that are usually quick

If a virus is running in the background on your computer, it may be using up system resources, which can cause other programs to slow down.

Frequent Crashes, Freezing, Blue Error Screens

Badly infected computers may frequently crash, freeze, and you may even see Windows crash completely and display a blue background screen with an error (these are sometimes referred to as "Blue Screens"). Blue Screen errors may have many causes, including a possible malware problem. Occasionally, badly infected computers may require more than a normal virus cleanup to return to normal operations.

Loss of Internet Connectivity

Malware is sometimes known to disable the internet connection on your PC. You might notice that your internet connection is unavailable when your coworkers are not having the same issue.

Browser Hijacking

One common type of malware is called a browser hijacker. This "hijacker" is designed to redirect your browser to potentially malicious websites. You might

Seltek offers a CLE seminar on "Retrieving and Using Electronic Evidence" approved for 1.0 hour of Virginia MCLE credit. To schedule, call Stephanie Greene at 804-360-4490 x13 or [by email](#)

To learn more about the computer forensics and e-discovery services of Seltek, Inc. go to

[Seltek Website](#)

notice that your homepage is suddenly different, or typing in certain web addresses (for example, google.com) do not bring up the correct webpage.

Pop Up Advertisements

Pop Up Advertisements are unfortunately common on many websites. They are not always a sign of malware. However, you may be infected if any of the following are true:

- There are pop up advertisements on websites that normally should not have them
- Multiple pop up advertisements with inappropriate content are being displayed
- You are experiencing a high number of pop ups when accessing the internet

Strange Programs and Rogue Antiviruses

Malware can cause strange programs or icons on your desktop to suddenly appear. This may also be evident when you open Internet Explorer and see new toolbars that were not there previously. Toolbars generally appear at the top of the browser window and sometimes have search windows, links or advertisements. They do not go away when you navigate to different web pages. Some toolbars are safe, such as Google and Yahoo, but some may be bundled with spyware or other malicious software.

Rogue antivirus programs have also become increasingly common.

These programs will appear on your PC when you have not purposefully installed them. Many act in different ways, including:

- Disabling your legitimate antivirus software (Symantec, McAfee, AVG, etc.)
- User is unable to uninstall the program
- Frequently appears to "scan" the computer and finds multiple "problems"
- Alerts the user that the PC is infected or unprotected until payment is sent

The purpose of these "rogue" antivirus programs is usually to alert the user that the PC is infected (when it may not be) and request payment for removal. These are scams. Some are designed to look like a Microsoft product, tricking the user into believing that it's part of Windows. Sometimes, they are so invasive that they restrict the user from opening any other programs, documents, etc.

If you suspect your PC is infected with a virus, call the Seltek Helpdesk at 360-4490 or [click here](#).



Try it FREE today.

This email was sent to carole@cytconsulting.com by wendy@seltekinc.com | [Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).
Seltek | 8814 Fargo Road | Suite 105 | Richmond | VA | 23229