

## Re: Security for 64 bit Vista Laptop

---

*Source:*

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.vista.security/2008-09/msg00083.html>

---

- *From:* Paul Montgomery <[i.m.nonnyonymous@xxxxxxxxxxxxxxxxx](mailto:i.m.nonnyonymous@xxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 11 Sep 2008 17:59:21 -0500
- 

On Thu, 11 Sep 2008 16:58:20 -0500, "James Colbert" <[jc2567@xxxxxxxxxxxxxxxxx](mailto:jc2567@xxxxxxxxxxxxxxxxx)> wrote:

Hi Kayman,

Thank you for a very comprehensive response! This is more than I could have asked for.

I've copied your post to my desktop for easy access to the URLs you have provided. I'll be chewing on this for a while! As for your last suggestion of regular defragging, I've been using Diskeeper for years, but not sure I want to buy another license. Is Vista's defrag utility adequate?

Definitely.

Still, I use Diskeeper. It gives me something else to play with ;-)

Thanks!

James

"Kayman" <[kaymanDeleteThis@xxxxxxxxxxxxxxxxx](mailto:kaymanDeleteThis@xxxxxxxxxxxxxxxxx)> wrote in message [news:e03g0d%23EJHA.6052@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:e03g0d%23EJHA.6052@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)

On Wed, 10 Sep 2008 20:17:29 -0500, James Colbert wrote:

I just picked up a laptop and am finishing the setup phase. I'll be installing Avast Anti-Virus, as I know it supports 64 bit and works reasonably well. Windows Defender is enabled, as is Windows firewall. Now I'd like to address strong security.

Re: Security for 64 bit Vista Laptop

Good combo!

If you ever look for a good (better IMO) AV alternative:

Avira AntiVir® Personal – FREE Antivirus

<http://www.free-av.com/>

(The free version won't scan your emails.)

Unless you are using Microsoft Outlook or Lotus Notes (MAPI or VIM), scanning email is worthless.

Why You Don't Need Your Anti-Virus Program to Scan Your E-Mail

<http://thundercloud.net/infoave/tutorials/email-scanning/index.htm>

Ensure your e-mail program is configured to display e-mail messages in 'Plain Text' only.

If you wish, you can remove the 'AntiVir Nagscreen'

[http://www.elitekiller.com/files/disable\\_antivir\\_nag.htm](http://www.elitekiller.com/files/disable_antivir_nag.htm)

In addition to WinDef you consider:

SuperAntispyware – Free

<http://www.superantispyware.com/superantispywarefreevspro.html>

This laptop will be used for business (and play as well, I suppose, especially during hurricane evacs).

Bad combo! Be very careful combining business with play :-)

One concern I have are for those times when I must download banking transactions into Quicken and Quickbooks. I'd like to be sure that my passwords and the sensitive data I'll be downloading is not accessible to anyone else. These downloads might take place via a hotel network or via a Sprint (or similar) broadband device.

Ensure that passwords are never stored on your operating system. Use an external media such as cd dvd or thumb drive.

Although my office is behind a hardware firewall, I really have no experience when it comes to 'on the road security'. Is it feasible to bring a router with a firewall to place between my laptop and the

## Re: Security for 64 bit Vista Laptop

hotel  
network,  
or should it all be handled by software (as I assume the case  
will be for  
the Sprint broadband).

There is nothing wrong taking your router and/or hardware firewall on the  
road as well.

I know that I am asking for more information than is  
probably practically  
posted here, but any information (including links) is greatly  
appreciated.

For Vista the most dependable defenses are:

1. Do not work in elevated level; Day-to-day work should be performed  
while the User Account Control (UAC) is enabled.

User Account Control Step-by-Step Guide.

<http://technet.microsoft.com/en-us/library/cc709691.aspx>

Understanding and Configuring User Account Control in Windows Vista.

<http://technet.microsoft.com/en-us/library/cc709628.aspx>

2. Familiarize yourself with "Services Hardening in Windows Vista".

Services Hardening in Windows Vista

<http://www.microsoft.com/technet/technetmag/issues/2007/01/SecurityWatch/>

Educational reading:

10 Immutable Laws of Security

<http://technet.microsoft.com/en-us/library/cc722487.aspx>

3. Don't expose services to public networks.

Windows Vista Service Configurations Introduction

<http://www.blackviper.com/WinVista/servicecfg.htm>

4. Keep your operating (OS) system (and all software on it)  
updated/patched. (Got SP1 yet?).

Windows update.

<http://www.update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us>

Secunia Personal Software Inspector

[http://secunia.com/software\\_inspector](http://secunia.com/software_inspector)

<https://psi.secunia.com/>

--And--

M/S Security Baseline Analyzer 2.0

<http://www.microsoft.com/downloads/details.aspx?FamilyId=4B4ABA06-B5F9-4DAD-BE9D-7B5>

can assist also.

Why Service Packs are Better Than Patches.

<http://www.microsoft.com/technet/archive/community/columns/security/essays/srvpatch.mspx?mfr=tr>

## Re: Security for 64 bit Vista Laptop

### 5. Secure (Harden) Internet Explorer.

IE7 safe/secure settings

Internet Explorer7 Desktop Security Guide

<http://www.microsoft.com/downloads/details.aspx?FamilyId=6AA4C1DA-6021-468E-A8CF-AF4A>

Internet Explorer Enhanced Security Configuration changes the browsing experience

<http://support.microsoft.com/default.aspx?scid=kb:en-us:815141>

The Internet Explorer 7 Security Status Bar

<http://www.microsoft.com/windows/products/winfamily/ie/ev/security.mspix>

Extended Validation SSL Certificates

<http://www.microsoft.com/windows/products/winfamily/ie/ev/default.mspix>

Note: \*Tight security settings will break down some websites. You need to add these websites into the Trusted Zone for smooth access.\*

You could consider disabling all Security Settings in IE and use IE only for the 'Patch Tuesday' updates; To do so you must add the following URL's to the Trusted sites:

<http://update.microsoft.com>

<http://download.windowsupdate.com>

[https://\\*.update.microsoft.com](https://*.update.microsoft.com)

[http://\\*.update.microsoft.com](http://*.update.microsoft.com)

[http://\\*.microsoft.com](http://*.microsoft.com)

### 6. Review your installed 3rd party software applications/utilities;

Remove clutter, \*including\* 3rd party software personal firewall application (PFW) – the one which claims:

"It can stop/control malicious outbound traffic".

### 7. Activate the build-in firewall and tack together its advanced configuration settings.

Tap into the Vista firewall's advanced configuration features

<http://articles.techrepublic.com.com/5100-10877-6098592.html>

"...once you discover the secret of accessing its advanced configuration settings via the MMC snap-in, you'll find it to be far more configurable and functional. At last, Windows comes with a sophisticated personal firewall that can be used to set up outbound rules as well as inbound, with

the ability to customize rules to fit your precise needs."

--Or--

Configure Vista Firewall to support outbound packet filtering

[http://searchwindowssecurity.techtarget.com/tip/0,289483,sid45\\_gci1247138,00.html](http://searchwindowssecurity.techtarget.com/tip/0,289483,sid45_gci1247138,00.html)

--Or--

Vista Firewall Control (Free versions available)

<http://sphinx-soft.com/Vista/>

### 7a.If on high-speed Internet connection use a router.

Re: Security for 64 bit Vista Laptop

7b. Implement countermeasures against DNSChanger.

<http://extremesecurity.blogspot.com/2008/06/use-default-password-get-hijacked.html>

7c. Just in case, Wired Equivalent Privacy (WEP) has been superseded by Wi-Fi Protected Access (WPA).

8. Utilize one (1) each 'real-time' anti-virus and anti-spy application.

9. Employ vital operating system monitoring utilities/applications.

Consider: Process Explorer, AutoRuns, TCPView, WALLWATCHER, Wireshark, Port Reporter etc.

10. Routinely practice Safe-Hex.

<http://www.claymania.com/safe-hex.html>

Hundreds Click on 'Click Here to Get Infected' Ad

<http://www.eweek.com/article2/0,1895,2132447,00.asp>

The least preferred defenses are:

Myriads of popular anti-whatever applications and staying ignorant.

Don't forget cleaning and defragging HDD frequently.

Good luck :)