

Re: Windows System Error: Spyware Detected

Source:

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2004-06/19635.html>

From: Bruce Chambers (*bchambers_at_nospamcableone.net*)

Date: 06/19/04

Date: Fri, 18 Jun 2004 20:36:37 -0600

Greetings --

It's a scam, plain and simple. It's from a very unscrupulous "business." They're trying to sell you patches that Microsoft provides free-of-charge, and using a very intrusive means of advertising. It's also demonstrating that your PC is very insecure.

This type of spam has become quite common over the past year or so, and unintentionally serves as a valid security "alert." It demonstrates that you haven't been taking sufficient precautions while connected to the Internet. Your data probably hasn't been compromised by these specific advertisements, but if you're open to this exploit, you most definitely open to other threats, such as the Blaster, Welchia, and Sasser Worms that still haunt the Internet. Install and use a decent, properly configured firewall. (Merely disabling the messenger service, as some people recommend, only hides the symptom, and does little or nothing to truly secure your machine.) And ignoring or just "putting up with" the security gap represented by these messages is particularly foolish.

Messenger Service of Windows

<http://support.microsoft.com/default.aspx?scid=KB:en-us:168893>

Messenger Service Window That Contains an Internet Advertisement Appears

<http://support.microsoft.com/?id=330904>

Stopping Advertisements with Messenger Service Titles

<http://www.microsoft.com/windowsxp/pro/using/howto/communicate/stopspam.asp>

Blocking Ads, Parasites, and Hijackers with a Hosts File

<http://www.mvps.org/winhelp2002/hosts.htm>

Whichever firewall you decide upon, be sure to ensure UDP ports 135, 137, and 138 and TCP ports 135, 139, and 445 are all blocked. You may also disable Inbound NetBIOS (NetBIOS over TCP/IP). You'll have to follow the instructions from firewall's manufacturer for the

microsoft.public.windowsxp.general: Re: Windows System Error: Spyware Detected

specific steps.

You can test your firewall at:

Symantec Security Check

http://security.symantec.com/ssc/vr_main.asp?langid=ie&venid=sym&plfid=23&pkj=GPVHGBYNCJEIMXOKCDT

Security Scan – Sygate Online Services

<http://www.sygatetech.com/>

Oh, and be especially wary of people who advise you to do nothing more than disable the messenger service. Disabling the messenger service, by itself, is a "head in the sand" approach to computer security. The real problem is not the messenger service pop-ups; they're actually providing a useful, if annoying, service by acting as a security alert. The true problem is the unsecured computer, and you've been advised to merely turn off the warnings. How is this helpful?

To deal with pop-ups caused by any sort of "adware" and/or "spyware," such as Gator, Comet Cursors, Xupiter, Bonzai Buddy, or KaZaA, and their remnants, that you've deliberately (but without understanding the consequences) installed, two products that are quite effective (at finding and removing this type of scumware) are Ad-Aware from www.lavasoft.de and SpyBot Search & Destroy from www.safer-networking.org/. Both have free versions. It's even possible to use SpyBot Search & Destroy to "immunize" your system against most future intrusions. I use both and generally perform manual scans every week or so to clean out cookies, etc.

Bruce Chambers

--

Help us help you:

<http://dts-l.org/goodpost.htm>

<http://www.catb.org/~esr/faqs/smart-questions.html>

You can have peace. Or you can have freedom. Don't ever count on having both at once. - RAH

"Scared_of_Spyware" <Scared_of_Spyware@discussions.microsoft.com>
wrote in message

news:F5B30E54-7AB5-4DD1-9408-0EA42EC30835@microsoft.com...

> In the past few days, I keep getting this pop-up that says, "Windows System Error: Spyware has been detected on your Computer." Then it says "click ok" to download this spyware remover program. Only, you have to pay for it. I know this is a bogus pop up, and adaware and spybot can't fix this. I tried looking for wierd programs and deleting them, but it won't work. Please help.