

Re: is it a virus? how to remove it?

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-08/msg00171.html

- *From:* Bruce Chambers <bchambers@xxxxxxxxxxxxx>
 - *Date:* Sun, 06 Aug 2006 09:40:23 -0600
-

s mishra wrote:

I'm using windows XP home edition with sp2. a pop up message is coming everytime i launch IE telling me that a security scan is required. I ran yahoo anti spyware and it removes some files. but the pop up keeps coming. any help?

What specific kind of pop-ups are you seeing? There are at least three varieties of pop-ups, and the solutions vary accordingly.

1) Does the title bar of these pop-ups read "Messenger Service?"

This type of spam has become quite common over the past few years, and unintentionally serves as a valid security "alert." It demonstrates that the computer user hasn't been taking sufficient precautions while connected to the Internet. The user's data probably hasn't been compromised by these specific advertisements, but if he/she's open to this exploit, he/she may well be open to other threats, such as the Blaster Worm that swept across the Internet years ago and the Sasser Worm that followed shortly thereafter, both of which can still be contacted. 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 the 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>

Oh, and be especially wary of people who advise the user 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

Re: is it a virus? how to remove it?

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 the user's been advised to merely turn off the warnings. How is this helpful?

2) For regular Internet pop-ups, you might try the free 12Ghosts Popup-killer from <http://12ghosts.com/ghosts/popup.htm>, Pop-Up Stopper from <http://www.panicware.com/>, or the Google Toolbar from <http://toolbar.google.com/>. Alternatively, you can upgrade your WinXP to SP2, to install IE's pop-up blocker. Another alternative would be to use another browser, such as Mozilla or Firefox, which has pop-up blocking capabilities. (But I'd avoid Netscape; it carries too much extraneous AOL garbage.)

3) 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.

Additionally, manual removal instructions for the most common varieties of scumware are available here:

PC Hell Spyware and Adware Removal Help
<http://www.pchell.com/support/spyware.shtml>

More information and assistance is available at these sites:

Blocking Ads, Parasites, and Hijackers with a Hosts File
<http://www.mvps.org/winhelp2002/hosts.htm>

The Parasite Fight
<http://www.aumha.org/a/parasite.htm>

Neither adware nor spyware, collectively known as scumware, magically install themselves on anyone's computer. They are almost always deliberately installed by the computer's user, as part of some allegedly "free" service or product.

While there are some unscrupulous malware distributors out there, who do attempt to install and exploit malware without consent, the majority of them simply rely upon the intellectual laziness and gullibility of the average consumer, counting on them to quickly click past the EULA in his/her haste to get the latest in "free" cutesy cursors, screensavers, "utilities," and/or wallpapers.

If you were to read the EULAs that accompany, and to which the

Re: is it a virus? how to remove it?

Re: is it a virus? how to remove it?

computer user must agree before the download/installation of the "screensaver" continues, most adware and spyware, you'll find that they _do_ have the consumer's permission to do exactly what they're doing. In the overwhelming majority of cases, computer users have no one to blame but themselves.

There are several essential components to computer security: a knowledgeable and pro-active user, a properly configured firewall, reliable and up-to-date antivirus software, and the prompt repair (via patches, hotfixes, or service packs) of any known vulnerabilities.

The weakest link in this "equation" is, of course, the computer user. No software manufacturer can -- nor should they be expected to -- protect the computer user from him/herself. All too many people have bought into the various PC/software manufacturers marketing claims of easy computing. They believe that their computer should be no harder to use than a toaster oven; they have neither the inclination or desire to learn how to safely use their computer. All too few people keep their antivirus software current, install patches in a timely manner, or stop to really think about that cutesy link they're about to click.

Firewalls and anti-virus applications, which should always be used and should always be running, are important components of "safe hex," but they cannot, and should not be expected to, protect the computer user from him/herself. Ultimately, it is incumbent upon each and every computer user to learn how to secure his/her own computer.

To learn more about practicing "safe hex," start with these links:

Protect Your PC

<http://www.microsoft.com/security/protect/default.asp>

Home Computer Security

<http://www.cert.org/homeusers/HomeComputerSecurity/>

List of Antivirus Software Vendors

<http://support.microsoft.com/default.aspx?scid=kb:en-us:49500>

Home PC Firewall Guide

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

Scumware.com

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

--

Bruce Chambers

Re: is it a virus? how to remove it?

Re: is it a virus? how to remove it?

Help us help you:

<http://dts-1.org/goodpost.htm>

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

They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.
–Benjamin Franklin

Many people would rather die than think; in fact, most do. –Bertrum Russell

.