

Re: Firewall

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-02/0682.html

From: Bruce Chambers (*bchambers_at_nospamcableone.net*)

Date: 02/05/04

Date: Wed, 4 Feb 2004 20:05:50 -0700

Greetings --

WinXP's built-in firewall is fine at stopping incoming attacks, and hiding your ports from probes. It doesn't give you any alarms to tell you that it is working, though. What WinXP also does not do, is protect you from any Trojans or spyware that you might download and install inadvertently. It doesn't monitor out-going traffic at all, much less block (or at least ask you about) the bad or the questionable out-going packets.

To enable the built-in firewall, Start > Network Connections > Right-click the connection > Properties > Advanced > Protect my computer.....

ZoneAlarm or Sygate are much better, and there are a free versions available. Personally, I've been very happy with Symantec's Norton Internet Security 2002 (NIS 2003 is now available), which includes Norton AntiVirus, Norton Personal Firewall, parental controls, privacy controls, and ad blocking. (Just the elimination of most pop-up ads on the Internet made the price worth-while to me.)

There are at least three varieties of pop-ups, and the solutions vary accordingly. Which specific type(s) is troubling you?

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

This type of spam has become quite common over the past several months, 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 may well be open to other threats, such as the Blaster Worm that recently swept cross 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 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

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?

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/>, which is what I use.

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.

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

"Pat" <anonymous@discussions.microsoft.com> wrote in message news:9eeb01c3eb27\$b338ec90\$a501280a@phx.gbl...

> I already have microsoft firewall installed, do I need to
> download anti-virus software from another company? If so
> what would you recommend, one that especially deals with
> those annoying pop-ups