

Re: Newbie -- how to make a broadband safe and secure???

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2004-05/0780.html>

From: Chuck (*none_at_example.net*)

Date: 05/21/04

Date: 21 May 2004 08:30:17 -0500

On 21 May 2004 05:27:59 -0700, *email_address_deleted* (Melanie C.) wrote:

*>I have a cable modem, I had to reinstall windows and I did not install
>any virus software before I went to do a Google search, ugggghh!!!
>
>I guess I have a Hijacker or something. I ran Norton virus scan but
>they remain there. I also now have McAfee's firewall...
>
>Does anyone know of a combination package or program that will keep
>everything safe, take all this crap and bots away, maybe a pop up
>blocker, spam blocker and something to make Only the programs that
>SHOULD be running, run?? Hmmm, maybe I am asking for too much?*

Melanie,

There is no all inclusive comprehensive package that will protect you from all the bad shit that hits the internet constantly. You'll need to create your own.

Try these free online virus scans, to verify the results from your installed protection:

<<http://www.bitdefender.com/scan/license.php>>

<http://www.pandasoftware.com/activescan/com/activescan_principal.htm>

<http://housecall.trendmicro.com/housecall/start_corp.asp>

Now check for, and learn to defend against, additional carriers of infection. Have you downloaded these programs before? Download them again, as many are revised frequently, to keep up with the current level of malware being attempted constantly – get the absolutely most current version of each product listed. They're all free – and most pretty small, so they download quickly enough.

First, download LSP-Fix and WinsockXPFix from <<http://www.cexx.org/lspfix.htm>>, and CWShredder from <<http://www.majorgeeks.com/download4086.html>>. All are free.

Next, close all Internet Explorer and Outlook windows, then run CWShredder. Have it fix all variants.

alt.computer.security: Re: Newbie -- how to make a broadband safe and secure???

Now check for, and remove, spyware. Get HijackThis

<<http://www.majorgeeks.com/download.php?det=3155>> and Spybot S&D

<<http://www.safer-networking.org/index.php?page=download>>. Both free.

1) Install and run Spybot. First update it ("Search for updates"), then run a scan ("Check for problems"). Trust Spybot, and make all recommended deletions.

2) Install and run HijackThis. Do NOT make any changes immediately. Save the HJT Log.

3) Have your HJT log interpreted by experts at one or more of the following forums (and post it here):

<<http://forums.net-integration.net/>>

<<http://www.spywareinfo.com/forums/>>

<<http://forums.tomcoyote.org/>>

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

If removal of any spyware affects your ability to access the internet (some spyware builds itself into the network software, and its removal may damage your network), run LSP-Fix and / or WinsockXPFix.

Finally, improve your chances for the future.

Harden your browser. There are various websites which will check for vulnerabilities, here are three which I use.

<http://www.jasons-toolbox.com/BrowserSecurity/>

<http://bcheck.scanit.be/bcheck/>

https://testzone.secunia.com/browser_checker/

Harden your operating system. Check at least monthly for security updates.

<http://windowsupdate.microsoft.com/>

Block possibly dangerous websites with a Hosts file. Three Hosts file sources I use:

http://www.accs-net.com/hosts/get_hosts.html

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

(The third is included, and updated, with Spybot (see above)).

Maintain your Hosts file with:

eDexter <http://www.accs-net.com/hosts/get_hosts.html>

Hostess <<http://accs-net.com/hostess/>>

Secure your operating system, and applications. Don't use, or leave activated, any accounts with names or passwords with trivial (guessable) values. Don't use an account with administrative authority, except when you're intentionally doing administrative tasks.

Use common sense. Yours. Don't install software based upon advice from unknown sources. Don't install free software, without researching it carefully. Don't open email unless you know who it's from, and how and why it was sent.

Educate yourself. Know what the risks are. Stay informed. Read Usenet, and various web pages that discuss security problems. Check the logs from the other components regularly, look for things that don't belong, and take action when

Re: Newbie -- how to make a broadband safe and secure???

alt.computer.security: Re: Newbie -- how to make a broadband safe and secure???

necessary.

And finally, Melanie, please don't contribute to the success of email address mining viruses. Learn to munge your email address properly, to keep yourself a bit safer when posting to open forums. Protect yourself and the rest of the internet – never post your address unmunged.

http://www.mailmsg.com/SPAM_munging.htm

Cheers,

Chuck

Paranoia comes from experience – and is not necessarily a bad thing.