

Re: Internet explorer

Source:

http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.network_web/2004-09/4652.html

From: Chuck (*none_at_example.net*)

Date: 09/28/04

Date: 28 Sep 2004 01:19:07 -0500

On Mon, 27 Sep 2004 20:29:28 -0700, "Eli" <anonymous@discussions.microsoft.com> wrote:

>I have windows xp. An unknown website is forcing itself
>every second time I'm trying to log to a website. I can't
>get rid of it. I tried to change the default website when
>I open explorer and again this "Bad" website change my
>default and a pop up about spy wear programs comes up. I
>have a spy wear program already and I can't get rid of
>this website or the pop up. HELP !!!!
> I tried to reset the settings in the computer to an
>earlier date but XP don't let me, because I already did it
>before. It is not succesful even if I choose a date later
>than the last restore. Thank You in advance for advise.

Eli,

I'm not sure what spyware program you already have, but browser hijacks are nasty stuff, and frequently require multiple products for detection and removal. HijackThis, and expert advice, is an essential tool.

Start by downloading each of the following free tools:

AdAware <<http://www.lavasoftusa.com/>>

CWShredder <<http://www.majorgeeks.com/download4086.html>>

CoolWWWSearch.SmartSearch (v1/v2) MiniRemoval

<<http://www.majorgeeks.com/download4113.html>>

HijackThis <<http://www.majorgeeks.com/download.php?det=3155>>

LSP-Fix and WinsockXPFix <<http://www.cexx.org/lspfix.htm>>

Spybot S&D <<http://www.safer-networking.org/index.php?page=download>>

Stinger <<http://us.mcafee.com/virusInfo/default.asp?id=stinger>>

Create a separate folder for HijackThis, such as C:\HijackThis – copy the downloaded file there. AdAware and Spybot S&D have install routines – run them. The other downloaded programs can be copied into, and run from, any convenient folder.

First, run Stinger. Have it remove any problems found.

microsoft.public.windowsxp.network_web: Re: Internet explorer

Next, close all Internet Explorer and Outlook windows, and run CoolWWWSearch.SmartSearchMiniRemoval, then CWShredder. Have the latter fix all problems found.

Next, run AdAware. First update it ("Check for updates now"), configure for full scan (<<http://www.lavahelp.com/howto/fullscan/>>), then scan. When scanning finishes, remove all Critical Objects found.

Next, run Spybot S&D. First update it ("Search for updates"), then run a scan ("Check for problems"). Trust Spybot, and delete everything ("Fix Problems") that is displayed in Red.

Then, run HijackThis ("Scan"). Do NOT make any changes immediately. Save the HJT Log.

<<http://forums.spywareinfo.com/index.php?showtopic=227>>

<<http://www1.spywareinfo.com/articles/hijacked/prevent.php>>

Finally, have your HJT log interpreted by experts at one or more of the following security forums (and please post a link to your forum posts, here):

Aumha: <<http://forum.aumha.org/index.php>>

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

Spyware Info: <<http://forums.spywareinfo.com/>>

Spyware Warrior: <<http://spywarewarrior.com/index.php>>

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

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/

Block Internet Explorer ActiveX scripting from hostile websites (Restricted Zone).

<<https://netfiles.uiuc.edu/ehowes/www/main.htm>> (IE-SpyAd)

Block known dangerous scripts from installing.

<<http://www.javacoolsoftware.com/spywareblaster.html>>

Block known spyware from installing.

<<http://www.javacoolsoftware.com/spywareguard.html>>

Make sure that the spyware detection / protection products that you use are reliable:

http://www.spywarewarrior.com/rogue_anti-spyware.htm

Re: Internet explorer

microsoft.public.windowsxp.network_web: Re: Internet explorer

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 (merge / eliminate duplicate entries) 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 layers regularly, look for things that don't belong, and take action when necessary.

Cheers,

Chuck

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