

# Re: Unwanted Web Pages keep opening up on IE

---

*Source:*

<http://www.tech-archive.net/Archive/WinXP/microsoft.public.windowsxp.general/2005-08/msg08684.html>

---

- *From:* "Kelly" <kelly@xxxxxxx>
  - *Date:* Mon, 15 Aug 2005 00:51:46 -0500
- 

You are missing a very important one:

Run Ad-Aware SE, Spybot and HijackThis:  
<http://www.majorgeeks.com/downloads31.html>

Note: Update the first two programs, once installed, before running.

--

All the Best,  
Kelly (MS-MVP)

Troubleshooting Windows XP  
<http://www.kellys-korner-xp.com>

"cquirke (MVP Windows shell/user)" <cquirkenews@xxxxxxxxxxxxxxxxxx> wrote in message [news:gtmuf110me8l297ahdg3tdsv0qd86h8rsh@xxxxxxxxxxx](mailto:news:gtmuf110me8l297ahdg3tdsv0qd86h8rsh@xxxxxxxxxxx)  
> On Sat, 13 Aug 2005 08:51:07 -0600, Bruce Chambers  
>>BH2 wrote:  
>  
>>> don't know what I have done but, web pages keep opening up when I  
>>> haven't  
>>> clicked a link. When I am on my computer not on IE, web pages keep  
>>> opening  
>>> up, the main ones are <http://ad.yieldmanager.com> and  
>>> [www.screensavers.com](http://www.screensavers.com)  
>>> how do I get rid of them. I have ad aware and spybot s&d, but do not  
>>> seem  
>>> to stop them, your help is appreciated  
>  
> I've used AdAware and Spybot as on-demand scanners; they may have some  
> "resident" protective facilities, but I haven't used those. This is  
> in contrast to traditional antivirus, which is best run as a resident  
> "underfootware" service, to intercept material as it tries to run.  
>  
> There's a third approach to malware, and that is static protection,

## Re: Unwanted Web Pages keep opening up on IE

- > such as applied by Spyware Blaster (and – unused by me – as part of
- > the Spybot feature set). This sets up certain settings in IE
- > Restricted Zone, browser cookie management, and the system-wide HOSTS
- > file, to block known offenders. Once again, this involves no code
- > running "underfoot", and thus no performance or stability impact.
- >
- > The final (first?) layer is the user. Think before you click:
- > – some web sites suck
- > – many sites found by a search will suck
- > – almost all that pop up unexpectedly will suck++
- >
- >> To deal with issues caused by any sort of "adware" and/or
- >>"spyware," such as Gator, Comet Cursors, Smiley Central, 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](http://www.lavasoft.de) and SpyBot Search & Destroy from
- >>[www.safer-networking.org/](http://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 is speaking from a time when commercial and traditional malware
- > were more clearly delineated than they are now. Yes, you certainly
- > will get more commercial malware if you click unwisely, but you can
- > get commercial malware without clicking anything at all – especially
- > if your system code is not patched properly.
- >
- > The three items that need continuous patching are:
- >
- > 1) Microsoft software, e.g. Windows, IE, OE, WMP, etc.
- >
- > I'm grouping these together because generally, the procedure to keep
- > these patched is similar, at least where those subsystems that were
- > bundled with the OS are concerned.
- >
- > Service Pack 2 tends to push a little too hard on this, IMO, in that
- > it will automatically install patches as well as downloading them; I
- > prefer to automatically download them, but review before installing
- > them. We've seen a couple of toxic patches that would have been
- > better avoided for a few days; unfortunately, we've also seen early
- > exploits that would have hit unpatched systems following that policy.
- >
- > 2) Firefox
- >
- > Like IE, Firefox is a large point of contact between your PC and the
- > outside world, and thus frequently needs patching to stay safe.
- > Microsoft releases such patches every month, and most months see a new
- > point revision of Firefox too.
- >
- > The patching process is different, though. Instead of downloading

## Re: Unwanted Web Pages keep opening up on IE

- > patches that repair unspecified parts of the large OS and interlinked
- > subsystems, with Firefox you simply download the new version (around
- > 5M) and install that over the existing one.
- >
- > 3) Java
- >
- > Many commercial malware (e.g. CoolWebSearch) attack defects in Java as
- > a clickless way into the system, so you need to patch that too.
- >
- > The process is similar to that of Firefox, i.e. you download an entire
- > new Java JRE and install it. It's a much bigger download, though.
- >
- > There's another important difference; whereas FireFox and MS replace
- > faulty code when installing the new version, Sun leave the older Java
- > engine(s) behind – and yes, they can still be exploited.
- >
- > So unlike MS and Firefox, you have to explicitly hunt down and kill
- > all older versions of Sun's Java, ideally before installing the new
- > one. I'd do MS and Firefox first, then Java, so that when Java asks
- > which browsers to integrate with, they are there to be chosen.
- >
- > <nice links snipped>
- >
- > The other thing that's changed, is that several traditional malware,
- > such as trojans and downloaders, are "rogue affiliates" that drop
- > commercial malware. Also, some things that appear to be commercial
- > malware turn out to be quite "rogue", in that no web site or other
- > accountable entity can be found.
- >
- > The result of all this, is that some things fall between the classic
- > "you have it because you installed it" commercial malware that
- > antivirus apps ignore, and that are safe to manage informally (e.g.
- > from Safe Mode), and the more hard-core stuff that enters without a
- > vestige of user permission, and which may defend itself in various
- > ways (disabling defences, running even in Safe Mode, etc.).
- >
- > So I've taken to approaching even commercial malware formally, i.e.
- > from a Bart PE CDR boot, as the first strategy. Fortunately, Spybot
- > works natively from Bart (the vendor offers a plugin for it, and it
- > has native supprt for inactive registry hives) and AdAware is fairly
- > easy to plug into Bart as well.
- >
- > In contrast, Microsoft's Antispyware Beta can't even install from Safe
- > Mode, let alone run "from orbit" (Bart's PE CDR boot). So while it's
- > an effective scanner, it's not as useful for first-contact
- > intervention; I use it after everything else has done most work.
- >
- >
- >>-----
- > Never turn your back on an installer program
- >>-----

- **Follow-Ups:**
  - ◆ **[Re: Unwanted Web Pages keep opening up on IE](#)**
    - ◇ *From: cquirke (MVP Windows shell/user)*
  
- **References:**
  - ◆ **[Unwanted Web Pages keep opening up on IE](#)**
    - ◇ *From: BH2*
  - ◆ **[Re: Unwanted Web Pages keep opening up on IE](#)**
    - ◇ *From: Bruce Chambers*
  - ◆ **[Re: Unwanted Web Pages keep opening up on IE](#)**
    - ◇ *From: cquirke (MVP Windows shell/user)*
  
- Prev by Date: **[Re: Why reply at the bottom of posts?](#)**
- Next by Date: **[Re: Why reply at the bottom of posts?](#)**
- Previous by thread: **[Re: Unwanted Web Pages keep opening up on IE](#)**
- Next by thread: **[Re: Unwanted Web Pages keep opening up on IE](#)**
- Index(es):
  - ◆ **[Date](#)**
  - ◆ **[Thread](#)**