

RE: DEP ALERT

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2006-12/msg00476.html

- *From:* jimmuh <jimmuh@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 26 Dec 2006 16:08:00 -0800
-

Hi. I'll try to be cogent, but I'm a little under the weather.

It is really important to distinguish between Windows Explorer and Internet Explorer (and, of course, other browsers).

You've said that you're using IE7, which is probably good. IE7 has the ability to help you control, to a very great extent, the behavior of any Add-ons (Browser Helper Objects / Browser Extensions) that you may have installed. Just go to the Tools | Manage Add-ons | Enable or Disable Add-ons location in IE7. There's a drop-down at the top of that dialog that lets you choose:

- Add-ons that have been used by Internet Explorer
- Add-ons currently loaded in Internet Explorer
- Add-ons that run without requiring permission
- Downloaded Active-X controls

You will need to look through those and study them to get a solid feel for what they are and where they come from. IE7 has an excellent online help file system. You'll want to use it to do your basic research and then look up your add-ons to be sure whether or not all of your add-ons should be there.

Windows Explorer can also have add-ons added to it. Popular ones do things like add toolbars or right-click context menu options. All such applications SHOULD put some kind of entry into your Add/Remove Programs dialog. Sometimes the entry in Add/Remove Programs has a name that isn't very similar to the name of what you installed. I wouldn't trust any installer that violates proper etiquette in this respect.

I suggest avoiding the addition to IE7 of things like download accelerators (Microsoft's own download manager is okay, though.) and things that control basic browser features like whether or not scripts will run. The browser is quite capable of handling all of this itself. And most, if not all, of these "enhancements" that I've seen are smoke and mirrors. You may need plug-ins to handle Flash, Adobe Acrobat, Quicktime, Real, and perhaps other popular online file formats. But adding anything that interferes with or supplements IE7's own control over its own internal functions is probably just asking for trouble.

RE: DEP ALERT

I'm concerned about your Java support. My Sun Java applet is Standard Edition 6 version 1.6.0 (build 1.6.0-b105) and was just downloaded from <http://www.java.com> yesterday. But I don't use the Sun JRE to support IE7. I install it (custom installation option) for use with Mozilla Firefox 2.0.0.1. I also use a plug-in named NoScript for Firefox. I turn off all scripting by default and enable it TEMPORARILY at each Web site I visit it on a case-by-case visit. That's how I browser everywhere but KNOWN good sites. I do my slumming with Firefox because that security arrangement just works better for visiting unknown sites --- in my opinion. But if you have an older version of the JRE installed that needs to be replaced right away.

You can turn off all scripting for ordinary Internet sites in IE7, too, and just add sites one-by-one to the Trusted category. That's a little less convenient and can result in a few odd issues with Windows / Microsoft Updates until you get it all sorted out.

I hope I haven't misunderstood your message and that my attempt at "advice" is not confusing. It is necessary for me to be a little vague here because it would be very hard for us to really nail down the exact configuration of your browser and all of the ramifications thereof. Basically I'm saying that you need to do some research and some real soul-searching on this issue of add-ons in this operating system. The Internet Explorer and Windows Explorer functions are integrated very tightly into the OS and can have far-reaching effects upon it. It is important to avoid installing anything for which you do not have a clearly demonstrated need. Even then, no matter how badly you feel you need a given function it is best to avoid installing it unless you have done some research to be sure that it is trustworthy. (Popularity of a piece of software is usually NOT a good criterion to use for establishing its trustworthiness, unfortunately.)

On my system I use Quicktime Alternative, Real Alternative, Adobe Flash, and Adobe Acrobat plug-ins for IE7. Those are the only IE plug-ins on my systems other than those that Microsoft actually provides with IE7 in Vista RTM. (I'm a TechNet subscriber and am using Vista Business for testing on my personal systems right now.) Any time I'm tempted to install something else I remember how many people I've helped people fix their systems after they installed "something else".

Good luck. And I hope my message isn't as muddle-headed as I feel.

"danny" wrote:

Thanks mate, You're right regarding the add ons for my browser which is IE7. I installed 'DAP' [download accelerator plus] the other day and now i can see the connection DEP, DAP its all coming together [smile]. And more recently, yesterday in fact, 'PopUpBuster' from ECOM software. Thereis an option in the setup of the latter to 'enable script links [Enables executing Java and VBScript links]' which i've just checked and it isn't enabled [unticked] which is the way it would have been at the time as I haven't changed it.

RE: DEP ALERT

— Iv'e just reread your reply and think I may have misunderstood. I don't know about anything placing extentions, add ons in windows explorer. PopUpBuster runs from explorer, is activated from win exp. Ther is no entry in 'all programs.

All I can tell you about Java is that it's Java 2 platform standard edition 1.5.0_b03.

Under browser settings, 'use browser settings is checked [on] which brings me back to Javascript support which I'm about to look into.

I've just realised that I had the address bar view on in win exp and also 'Answers.com' is this what you was getting at? [sorry if this is a bit jumbled]

Anyway thanks for your help and might I recommend 'Percol' coffee it kickstarts me every morning.

"jimmuh" wrote:

The DEP message you received may, or may not, have been related to the Web site for which you received a warning.

I have two suggestions to make, and I hope others will chime in if there are other matters I'm overlooking.

First, since you mentioned a recent update to "Java" (Javascript?) specifically, as well as a warning while visiting that Web site — which browser, and which Javascript support for it, were you using? For normal browsing to sites with unknown characteristics I strongly suggest NOT enabling scripting in the browser (regardless of brand or version of the browser). Enable scripting ONLY for sites that you trust on a one-by-one basis. This is accomplished by different methods in different browsers. You don't want to get a step-by-step for this from someone on a newsgroup. You want to do the research yourself so that you understand how and why your browser works the way it does. But the bottom line is — no active scripting allowed unless YOU specifically allow it for the site you are visiting.

Regardless of which browser you are using always make sure that your Javascript support is up-to-date. A good general overview of security issues that covers all of the common software sources is the Secunia security advisory. There are others. Subscribe to one via RSS or e-mail. Read every issue to be sure that you have applied patches or workarounds for every item that applies to your systems. There have been fairly recent updates to the Microsoft scripting support for its browsers and for the Sun JRE, which supports other browsers like Firefox as well as IE.

Regarding DEP closing Windows Explorer (not Internet Explorer), if I understood your message correctly this is what happened to you, and I suspect that it probably doesn't have anything to do with the Web site you mentioned — unless you installed something from that site on your system. (Some of

RE: DEP ALERT

the techniques used for getting us to install stuff can be pretty insidious.)

But I'm guessing that you have an application installed that places an extension or add-on in Windows Explorer. I can give you an example with which

I have personal experience. In Windows XP Pro SP2 I kept receiving occasional

Windows Explorer shutdown messages from DEP. I finally traced it to an application named SnagIt which installed a plug-in or extension for Explorer.

All I had to do to eliminate the issue was to tell the SnagIt installer NOT to install that context handler -- or remove SnagIt altogether. Because SnagIt's plug-ins were also causing problems with some Office apps I just blew SnagIt off the system --- though I had used it for years. I found other ways to get the functionality I needed. Pretty easy to do in Vista RTM.

I think you need to check to see if you have something on your system that adds extensions to Explorer. Eliminate all such items temporarily, see if the problem occurs again. If not, add them back until it does. You might also extend DEP to cover all applications, rather than just the Windows components

that it covers by default. That's what I do. That setting may warn you about behavior from an application which could cause failures in Explorer or other Windows components.

Sorry for the rambling. Not enough coffee yet this morning.

"danny" wrote:

I got a message from DEP [data execution protection] telling me that it had to close win exp for security reasons so as well as doing this I clicked the link for help on this subject. It explained the steps to take if DEP takes action and these were pretty standard security measures [scan etc] It also said something about when it is ok to use the affected app again but being windows explorer I don't see as I have a choice. My AVG had just done its scheduled scan and come up with nothing and i have used win exp since with no problems so is it possible this was a glitch or something? The only possible breach of security I can think of is last night 'java' gave me a security warning about a web site whilst browsing. It gave me the option to either

RE: DEP ALERT

continue to the site or cancel, i cancelled but still appeared to go to the site. I have just updated java and AVG is up to date too. Any light shed on this would be much appreciated thanks.

PS MERRY CHRISTMAS

—

hodcarrier,carp