

## Re: Safe?

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-06/1441.html>

---

**From:** YK ([YKnot\\_at\\_home.invalid](mailto:YKnot_at_home.invalid))

**Date:** 06/26/03

Date: Thu, 26 Jun 2003 11:07:29 -0400

Johnny wrote:

- > *I am running XP Pro and I always have the latest service*
- > *packs installed. I also use Norton Internet*
- > *Security/Antivirus with all the latest definitions. is*
- > *this enough to protect my PC from hackers? What sort of*
- > *security risks don't I know about?*

Answers to the Ten Most Frequently Asked Questions in  
microsoft.public.security newsgroups.

Read Q5

Read Q11 as well.

=====

Q1) I got an email from Microsoft about a security update. Should I run the attachment?

A1) No. Microsoft NEVER sends emails with security update attachments. You can subscribe to mailing lists to receive Microsoft security bulletins or read Microsoft security bulletins on the web. These bulletins NEVER contain executable attachments, only references to web pages where you can access Windows Update, download patches, or request to receive patches from Microsoft Product Support Services. You should never use any tool other than Automatic Updates, the Windows Update web site, or a response to your request to Microsoft Product Support Services to install Windows security updates or hotfixes.

See [http://www.microsoft.com/technet/security/news/patch\\_hoax.asp](http://www.microsoft.com/technet/security/news/patch_hoax.asp) for an explanation from Microsoft about these hoax email messages.

=====

Q2) I got an email telling me I should remove the  
Teddy Bear virus  
that is contained in a file named jdbgmgr.exe.  
Should I follow these instructions?

Re: Safe?

microsoft.public.security: Re: Safe?

A2) No. This file is a Microsoft java debugger file. Do not remove it. If you do remove it, you needn't bother to restore it, since it is likely you won't ever need it.

In general, DO NOT follow instructions in unsolicited emails from sources you do not know and should not trust.

=====

Q3) I read a newspaper article some time ago and followed a link from the article and found myself here. How do I get help here? What is this place?

A3) You are in what is known as a Microsoft community or a Usenet

newsgroup, or simply netnews.

Go to <http://communities.microsoft.com/home/newscat.asp> to see all the Microsoft newsgroups available on the Microsoft news servers at msnews.microsoft.com. Also read about which newsreaders you can use at <http://www.microsoft.com/communities/guide/newsgroups.mspx>. I recommend using Outlook Express because you can be notified of new newsgroups when they are added by Microsoft, you can watch your posts and see your responses highlighted, and you can more easily create posts.

You should read about proper posting etiquette at <http://dts-l.org/goodpost.htm>. Before you post a question to a Microsoft.public.\*.security newsgroup, you should read the following collection of answers to common questions:

<http://securityadmin.info/faq.htm>

=====

Q4) What is the best way to stay up-to-date with Microsoft security updates?

A4) In Windows XP, open your System control panel to the Automatic Updates tab. You can enable download and install separately, according to your preferences.

You may also subscribe to Microsoft Security bulletins which will arrive in your email at about the same time as AU notifies you of available updates. Sign up to receive the security bulletins in email at [http://www.microsoft.com/security/security\\_bulletins/decision.asp](http://www.microsoft.com/security/security_bulletins/decision.asp). Before installing any Windows patch/hotfix/update, you should read the bulletin, either in your email or on the web at [http://www.microsoft.com/security/security\\_bulletins/archive.asp](http://www.microsoft.com/security/security_bulletins/archive.asp). If you have any doubts about the necessity or safety of the update after reading the bulletin, delay the install and read the security newsgroups

Re: Safe?

microsoft.public.security: Re: Safe?

over the next couple of days to see if there are any problems with the recent update. There is always a thread, usually with the KB article number (a six digit number, sometimes preceded by a Q) in the subject line, discussing any problems with the most recent updates.

You should also visit Windows Update regularly. There is a Windows Update item in Internet Explorer under Tools and you can often find a shortcut at the top of the Start Menu or go to <http://v4.windowsupdate.microsoft.com/en/default.asp>. Windows Update provides the same security updates and provides additional recommended updates that are not offered by Automatic Update.

If you are an enterprise, you may also use the new Microsoft Software Update Services server software to provide updates within your organization. You can find additional information regarding Microsoft Software Update Services (SUS) at <http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp>

=====

Q5) How can I know if my system is secure? How do I know if I have all the right patches from Microsoft installed? Can I test my system security?

A5) You cannot really know how secure your system is, except that you watch for reports of vulnerabilities in the news or in Microsoft bulletins and keep up-to-date on your critical updates to Windows.

There are two tools that you can use to test whether your system is up-to-date with Microsoft security updates. These are the Microsoft Baseline Security Analyzer and the Microsoft/Shavlik hotfix checker.

Learn about the MBSA tool at <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp>

The MS hotfix checker can be downloaded at <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/hfnetchk.asp>

Note that these security checkers are unable to verify non-security related updates. The most common result is a note that states that a file version number is greater than expected. This note is normal and results from other Microsoft recommended updates that update these files to newer versions. See <http://support.microsoft.com/?id=306460> for more information on hotfix checker notes. Also note that hotfix means the same thing as security update.

Another aspect of system security is how well your Windows is configured for on-line security. Your system may be vulnerable to attacks via services that you don't actually need to run that leave unnecessary ports open. You may scan your system for online vulnerabilities using a non-Microsoft service from a third-party web site. Go to

Re: Safe?

microsoft.public.security: Re: Safe?

<http://www.grc.com/> and find the free tool called Shields Up at <https://grc.com/x/ne.dll?bh0bkyd2>. Also see <http://security2.norton.com/> for another port scanner that will test your Internet security.

=====

Q6) I keep getting windows popping up on my system, even when I am not using Internet Explorer, that tell me my system is vulnerable and I need to buy some software. Some of the windows are other sorts of advertisements. How can I stop these pop-ups?

A6) These windows are sent to your system using the Messenger service. You should use a firewall to block your file/printer sharing ports (TCP/UDP ports 135, 137, 138, 139, and 445) from the Internet. Or you can disable the Messenger service (not Windows or MSN instant Messenger) using services.msc on Windows 2000 or XP but this still leaves your system visable on the Internet.  
<http://www.firewallguide.com/>

See also Q9)

=====

Q7) Windows Update has a problem. How do I fix it?

A7) Go to <http://v4.windowsupdate.microsoft.com/troubleshoot/> to find solutions to common Windows Update problems.

=====

Q8) How can I read an attachment which I know is safe, but Outlook Express 6 has denied access to me?

A8) Go to Tool, Options, Security tab and uncheck the box labeled Do not allow attachments to be saved or opened that could potentially be a virus. Attachments that you could not save or open will now be available. This is a new feature of OE6SP1. Be careful. Some attachments really are dangerous and they may come from someone you know, if that friend has a virus that sends dangerous email attachments. You should save the attachment and then manually scan it with an anti-virus tool before opening it. See the Microsoft article at <http://support.microsoft.com/?kbid=329570> for more information on this subject.

=====

Q9) How can I tell if I have spyware or other malicious software on my system and how can I get rid of it if I have it?

Re: Safe?

A9) Spyware, trojans, viruses, snoopers, and other types of malicious software are often hard to detect when present. Your computer may slow down, Windows Explorer may crash frequently, your Internet access may be slow or unavailable, and you may get unexpected error messages when trying to open programs. Viruses, trojans, and worms are software that install themselves secretly and without your permission and replicate themselves from your system to other systems. Spyware are software that install themselves with your often unknowing but explicit permission. They do not usually replicate themselves.

There are two types of tools to remove viruses and spyware.

An anti-virus tool protects your system from viruses, worms, and trojans that infect your system without your permission and replicate themselves to your unfortunate friends and associates and embarrass you in the process. These malicious uninvited programs are sometimes quite dangerous, if not to you, then to others you may infect or unknowingly attack. Some viruses will install attack software on your system, making your computer an unwitting accomplice in a malicious and damaging attack against someone else, as directed by the virus distributor. You have a responsibility to protect your system against these threats in order to protect your friends, other Internet users, and valuable web sites on the Internet against coordinated, massive denial-of-service attacks from virus-infected machines. You are particularly vulnerable to these infections if you have a broadband Internet connection. Norton/Symantec, McAfee, and Trend Micro make good anti-virus products for sale. AVG by Grisoft is free for personal use.

An anti-virus scanner cannot protect your system from spyware that you deliberately, but unknowingly, install on your computer when you or someone who uses your computer downloads and installs free software from the Internet. Therefore, you need a spyware scanner to remove these mildly malicious programs that spy on your Internet behavior, pop-up unwanted and intrusive ads when you browse the Internet, hijack your home page, hijack web sites, and slow down and crash your system. Note that removal of spyware will sometimes disable the free software from which the spyware originated. The license agreement you failed to read usually explains what software is being installed and whether it is necessary to use the free program that you really want. There are sometimes versions of free software available without the spyware.

The best spyware removal tools are Adaware available from <http://www.lavasoft.de/software/adaware/> or <http://www.lavasoftusa.com/software/adaware/> and Spybot available from <http://tomcoyote.org/~mosaic1/spybot/> and update the reference file through the Online update function. Run it and select all items and remove.

You may have to reboot and rerun a couple of times to completely remove it. Also run the Immunize function to prevent these nasties from installing again.

Install a good HOSTS file.

Blocking Ads with a Hosts File and AdShield. Under the Security Tab download the hosts.zip file.

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

=====

Q10) Does Windows have a firewall or an anti-virus scanner? If so, how do I turn them on. If not, do I need these tools and where can I find some free ones?

A10) Windows XP is the first version of Windows to provide a firewall, called the Internet Connection Firewall or ICF. You can enable ICF from the connection properties on the Advanced tab. You cannot configure or tweak the built-in firewall, it is either on or off. ICF blocks many incoming port scans as well as Microsoft file and printer sharing, so you shouldn't use it on a network behind a NAT router or other firewall, as you will be unable to share files and printers in a workgroup if ICF is enabled.

ICF does not monitor outbound originating traffic. If you want to monitor outbound traffic for spyware activity, you need a third-party product like ZoneAlarm available from <http://www.zonelabs.com/>, SyGate Personal Firewall from [http://soho.sygate.com/products/shield\\_ov.htm](http://soho.sygate.com/products/shield_ov.htm), or Kerio WinRoute Firewall at [http://www.kerio.com/kwf\\_home.html](http://www.kerio.com/kwf_home.html). You can do a simple one-time web anti-virus scan at <http://housecall.trendmicro.com/>. But remember that whatever tool you get, to be able to use it effectively, you must keep the virus definitions database up-to-date.

Windows does not provide any anti-virus tool, but your system may have an anti-virus scanner installed by your computer maker. There are many anti-virus tools available. One free anti-virus scanner is AVG available from <http://www.grisoft.com/>. Anti-virus tools are useless without frequent updates, so be sure to check the date on your anti-virus data file and update at least once a month or whenever you run a full scan.

Note that there are problems with some versions of Windows and Outlook Express and some anti-virus background and email scanners, so be advised that if you enable automatic anti-virus protection and experience problems, you will need to seek help here to resolve those issues. This is not a recommendation to avoid automatic anti-virus protection, simply a warning that there are problems with several anti-virus tools in this respect.

=====

Q11) I have a question that you haven't covered in this list. How do I find an answer? Must I create a post in the newsgroup?

microsoft.public.security: Re: Safe?

A11) No, you shouldn't post until you have searched a few well-known sites for answers to your question. Go to [http://www.google.com/advanced\\_group\\_search](http://www.google.com/advanced_group_search) and <http://www.microsoft.com/support/> to input your questions.