



October 6, 1998
Volume 2, Issue 1

PC Tips On-Line
www.powerturn.com/goodies.html

Inside This Issue

- 1 Email Security Alert!
- 1 When Is A Virus Not A Virus?
- 2 An Ounce of WSH Prevention
- 2 Keyboard Shortcuts
- 2 This Issue's URLs*

Madeline A. Lombaerde
PowerTurn Consulting
Voice: 650/592-5464
Fax: 650/299-0653
mal@powerturn.com
www.powerturn.com

PC Tips

Email Security Alert!

Thanks to a bug and a feature, it is now possible for an email message to cause damage to your computer and possibly your network.

Message Safety No Longer True

Previous publications, including the April 24, 1998 issue of PC Tips, have stated that you can't get a virus from an email message itself, just from an attachment and only when the attachment itself is opened. *That is no longer true.* Under certain circumstances, you *can* get a virus just by opening an email message or from a message that has an attachment with a long filename *even if you don't open the attachment!* You can also be attacked just by browsing a Web page.

Virus Risk: Reading Email Message

A Microsoft utility called Windows Scripting Host (WSH) was designed to give administrators and other users a way to automate tasks done on a routine basis. However, Outlook 98 and Outlook Express can interpret WSH scripts, which means that commands can be easily added to an email message which could delete files and folders or do other malicious things to the recipient's system. When the message is read, the commands are interpreted and executed.

Are You At Risk?

If your Windows 95 or NT system has version 3.1 of WSH installed, you are at risk. Internet Explorer 3.02 will run the deadly scripts with no warning. IE4 will at least alert the user that the script in the message or web page may be dangerous. Netscape users are not at risk: Netscape

Navigator and Mail don't execute WSH scripts. See the [article on WSH protection](#) for details on how to protect yourself from dangerous scripts.

Virus Risk: Unopened Attachments

A bug that is present in various email programs allows a hacker to send a message with an "attachment" that has a very long filename. The filename can actually contain code that can damage a recipient's system just by receiving the email, regardless of whether the attachment is opened. There is a patch for this problem. If you use Outlook 98, go to <http://support.microsoft.com/support/kb/articles/q175/8/07.asp> for more information about the problem and the patch. *Note:* Microsoft requires that you register with them to get articles from the Technical Support Area.

For Outlook Express, see <http://support.microsoft.com/support/kb/articles/q168/0/19.asp>

If you use Eudora Pro 4.0 or 4.0.1, go to http://eudora.qualcomm.com/pro_email/updaters.html to upgrade to a version that eliminates the problem. For details about the Eudora Pro security problem, see <http://eudora.qualcomm.com/security.html>

When Is A Virus Not A Virus?

When it is a **hoax**. Hoaxes are warnings about viruses that don't exist. They are usually spread via email and newsgroups. Well-meaning people then compound the problem by forwarding the warning to all their friends. The result is millions of unnecessary messages taking up valuable transmission bandwidth, clogging email servers and user computers around the world, and causing unwarranted alarm,

especially in people new to computers and the Internet.

Avoid Spreading Hoaxes

Please don't forward a virus warning to even one friend before you first check to see if the warning is a hoax. I always go to the Symantec Anti-Virus Research Center's hoax list page found at <http://www.symantec.com/avcenter/hoax.html> to determine if the warning is valid or is a hoax. Other anti-virus centers have similar lists. If you receive a hoax from a friend, let them know about the Hoax list page so they can check it before passing on such messages.

An Ounce of WSH Prevention

WSH (see Email Alert! article in this issue) allows VBScript or JavaScript to be executed from a command line or from a Windows shortcut. WSH uses the VBScript engine and a problem in the 3.1 version of VBScript surfaced in December, 1997. Outlook 98 and

Outlook Express can run VBScript, so it became possible for malicious scripts to be passed in email messages. To find out if you have this problem, check your Windows system folder to see if you have a file called VBSCRIPT.DLL dated 12/30/97 or later and the version is 3.1a.

Find the VBScript Version

To do this, open Windows Explorer, go to your windows system folder (C:\windows\system) and look for VBSCRIPT.DLL. If you are in icon view, click VIEW > DETAILS. If the date is 12/30/97 or later, right-click on the file name and choose Properties. Click on the Version tab. If it is 3.1a, you are vulnerable. You can either tighten security or disable the feature completely.

Tighten Security with IE4

If you are running IE 3.02, upgrade to

the latest IE 4. If you prefer to not upgrade, you'll have to disable the feature. If you are running IE 4, tighten security as follows: Run IE4, choose View>Internet Options>Security (tab). Click on the Custom option, then the Settings button. Disable the option "Initialize and Script ActiveX Controls Not Marked As Safe". Do not leave it set to Prompt! Do the same for Outlook 98 and Outlook Express: choose Tools>Options and go to the security zone settings.

Disable Scripting Feature Completely

To completely disable the Windows Scripting Host feature, find the file named SCRRUN.DLL and delete it. Web-based scripts will continue to work but they won't have access to your files or folders.

For More Technical Information

PC Computing, July 1998, has a great article on the WSH problem. See "You've Got (Deadly) Mail" on page 42.

Keyboard Shortcuts

Want to move around a document quickly? Try the following the next time you're in Word 97 or Notepad or any modern Windows word processor:

Ctrl + Home

move to beginning of document

Ctrl + End

move to end of document

Home

move to beginning of line

End

move to end of line

[Ctrl + *key* means hold the Control key down and press the specified *key* once.]

To *select* text, use the Shift key:

Ctrl + Shift + Home

Select to beginning of document

Ctrl + Shift + End

Select to end of document

This Issue's URLs*

Outlook 98 Security Issue & Patch

Information on long filename attachment security issue and patch for Outlook 98.

<http://support.microsoft.com/support/kb/articles/q175/8/07.asp>

Outlook Express Security Issue & Patch

Information on long filename attachment security issue and patch for Outlook Express.

<http://support.microsoft.com/support/kb/articles/q168/0/19.asp>

Eudora Pro Security Issue & Patch

Information on long filename attachment security issue and patch for Eudora Pro 4.0 and 4.0.1.

<http://eudora.qualcomm.com/security.html>

Virus Hoax List Page

Find a list of the currently known hoaxes being spread around the Internet. Let your friends know about this page!

<http://www.symantec.com/avcenter/hoax.html>

Symantec Anti-Virus Research Center

Great resource for finding out about the latest viruses and hoaxes. Download latest definition list if you use Norton Anti-Virus.

<http://www.symantec.com/avcenter/index.html>

*URL: uniform resource locator. WWW jargon for the address of a Web page.