Protecting against Viruses with Outlook

Using Microsoft Outlook is an open invitation to virus writers. The same tools that Microsoft has put in place to allow for increased automation and flexibility are those used by virus writers to spread e-mail viruses and worms (such as I Love You and the Anna Kournikova worms). Since Microsoft considers its susceptibility to viruses a "feature" it is unlikely to make any structural changes that would remedy the situation. The Microsoft "Security Patch" does stop some of these viruses, but it also prevents Outlook from functioning properly with third party programs such as case management or Palm Pilot synchronization. The best source of information on these matters is Woody Leondard's "Woody's Office Watch" (at www.woodyswatch.com).

The two main lines of defense, as always, are training and proper virus protection.

Train users never to open an attachment unless they know it is coming, even if it is from someone they know. Many viruses spread by sending themselves to the first 50 or so addresses in the infected party's address book. Therefore you can get a virus "from" someone you know that is being sent without their knowledge. Always save the file and view it with a viewer before opening it. Some newer viruses can execute when a file is viewed in the Outlook viewer pane, so that is no longer adequate protection. As a general practice, you should keep the viewer pane closed at all times.

Keep your anti-virus software updated. You should update your software at least once a month and once a week if you have a software that will do updates automatically.

There are four additional steps you can take that will substantially cut down on viruses.

☞ Always turn on extensions and show all files (*.exe, etc.). Some viruses use double extensions, such as anna.jpg.vbs. Unless you turn on extensions, that file would appear to be a simple graphics file: Anna.jpg. (The *.vbs file indicates that it is a Visual Basic file which is the language many viruses are written in.)

☞ Change the *.vbs file association to Notepad, so that any vbs script files will open in notepad and not execute. To do this, right-click on "My Computer" and select "Explore." Select View | Folder Options. Click on the "File Types" tab and scroll down to the "VB Script" options. Change them so that the association is Notepad.exe, not wscript.exe.

☞ Rename the two files that are generally used by viruses to execute. These are: c:\windows\wscript.exe and c:\windows\command\cscript.exe. Note: it is possible (but not too likely) that this may disable some other functionality. After you do this, keep an eye on your system for a week or so to see if you suddenly get strange error messages related to VB Script.

Taken together, these steps will seriously reduce your exposure to viruses when using Outlook.

Follow Suggestions in Woody's Office Watch

People whose clients are using Outlook and other MS products would do well to follow Woody's Office Watch (at www.woodyswatch.com). For information concerning the recent disastrous Outlook "security" patch - which disables integration with Time Matters and many other 3rd party products see in particular the WOW Newsletters 5.24 through 5.26. I find this weekly newsletter indispensable. They have a much superior patch for Outlook which a) lets you choose what functions you want to patch and b) let's you undo the patch if you change your mind. The MS patch does neither and if you change your mind the only solution is to uninstall Outlook and re-install it. Here is an extensive quote from the newsletter:

> "Microsoft should make an announcement that in response to complaints it has received (and believe me, the affected ISVs and most MVP who have actually seen the patch are yelling about it), it has decided to postpone release of the patch until it can get it right. It should then focus on a patch that only does 1 and 2 and adds the dialog boxes to 2 to make it easy to customize. If it can find a way to place the address book off limits without being intrusive, it could be added AS AN OPTION.
>
> "But if Microsoft persists and releases this awful, terrible, dysfunctional, dreadful, appalling, atrocious, horrendous, inexcusable patch, you should not use it yourself and you should tell all your friends not to consider the patch. I'll bet almost no one at Microsoft uses it! " In particular, warn any IT types that you know to exercise especial care since the only way to undo this patch is to uninstall and reinstall Office! As to how you can defend yourself without the patch, in the next WOW, I'll provide some work-arounds including a Registry file to accomplish what 1 of the security patch does. For now, you can consult http://www.slipstick.com/outlook/antivirus.htm."