

Cleaning up your inbox

OFTEN OUR INBOXES seem to contain more in the way of viruses, spam and other junk than emails we actually want to read. If your email is becoming a nuisance, then it may be time to consider the features of Outlook 2002 that can help make your inbox a much nicer (and safer) place to visit. David Peterson reports

The antidote to viruses

There are two main ways that viruses can be transmitted via email:

- 1) The most common is a virus-infected attachment with an enticing name which, when opened, unleashes the virus on your computer.
- 2) HTML email can contain scripts that will execute malicious code even if you only read the email or open it in the preview pane.

Fortunately, Outlook 2002 will automatically protect you from most email nasties by blocking suspicious attachments and scripts. To provide an additional level of protection, however, it is recommended that you adopt the following best practices for email safety:

- 1 Use **Tools > Options > Security** to make sure that the security zone for Outlook HTML email is set to 'Restricted Sites'.
- 2 Visit the Microsoft Windows Update and Office Update Web sites to check that you are using the latest versions of Outlook and Internet Explorer with all the latest service packs and security updates.
- 3 Never open an attachment that you didn't expect to receive. If in doubt, email the sender for confirmation.
- 4 Make sure that you know what type of file is attached to an email. Some viruses disguise themselves with double file extensions like .jpg.vbs – so if you have set Windows to hide the file extension for known file types you would see the attachment listed as a harmless .jpg file rather than as a potentially dangerous .vbs file. Make sure that you can see the extensions for all files by using **Tools > Folder Options > View** from any window in Windows Explorer and unchecking 'Hide file extensions for known types'.

For the particularly security conscious, the GFI Email Security Testing Zone (www.gfi.com/emailsecuritytest)



provides a free audit service – sending you harmless email messages that test a range of email vulnerabilities.

Canning spam

Outlook has built-in spam filtering that can be switched on using the 'Organize' function accessible from the toolbar or from the Tools menu. Of course, most spammers already know about these filters and deliberately write their spam emails to circumvent them. Fortunately, in Outlook 2002 you have an additional line of defence with the Outlook Rules Wizard.

The Rules Wizard is a powerful and flexible tool

that lets you determine how Outlook will treat emails based on their sender, content and a number of other characteristics. An obvious application of this is blocking undesirable emails. For example, to add a new spam-blocking rule in Outlook:

- 1 Select Rules Wizard from the Tools menu in Outlook.
- 2 Click the New ... button to create a new rule.
- 3 Make sure that 'Start creating a rule from a template' and 'Move messages based on content' are selected.
- 4 Click 'specific words' to add a list of keywords you have commonly found in spam messages.
- 5 Click 'specified folder' to select where you would like the emails redirected (see Figure 1).

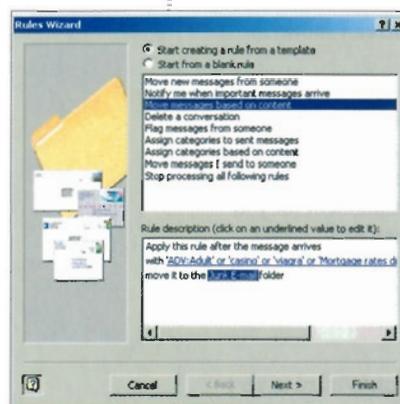


Figure 1

Filtering spam is just one of many uses for the Outlook Rules Wizard. I'll be covering some of the others in next month's Netsmarts column.