



E-Mail Lockdown

By Gregg Keizer,

August 21, 2006 (12:00 AM EDT)

URL: <http://www.techweb.com/tech/192201948>

E-mail is second only to Web browsers as an avenue for attack. Following are five steps to lock e-mail against common threats, including phishing campaigns, spam that bears Trojan horses, and ploys to get users to visit infectious Web sites. These steps are primarily recommended for Microsoft Outlook but in many cases can be applied to other e-mail programs.

PREVIEW NO MORE Some malignant messages need only be viewed to do damage. An e-mail client's preview pane--the part of the display that shows a portion of a message when you point your cursor on it--is a time-saver, but users who turn off the panel option will be better protected. That provides the chance to decide if the sender of a message is a trusted source by viewing the subject line before opening a message and exposing its content.

GO PLAIN VANILLA Attackers also are creating HTML-based e-mails that need only be viewed or opened to cause damage. Generally, these attacks are exploiting a vulnerability in the e-mail client and/or the browser through an HTML script. One way to stymie such attacks is to select plain text for viewing e-mail instead of HTML. (Another nonsecurity reason to take this step is to eliminate the fancy ads that populate some spam.)

LOSE THE LINKS Phishing attacks rely on enticing users to click on links to dubious Web sites; increasingly, so do more malicious assaults. Make it more difficult to click on to these links by disabling every HTML link that arrives. The links will still exist, but users won't be able to click on them to open the browser and surf to the site. Temptation removed.

STAY UNATTACHED Everyone knows you're not supposed to click on attachments from an unknown sender, but attackers are getting better at looking like trusted sources, tricking users into clicking before they think. Microsoft Outlook has an attachment-blocker feature that prevents users from opening a long list of file formats and from saving potentially dangerous files to hard drives from within Outlook. This feature is standard in Outlook 2002 and 2003; earlier versions require a patch available from Microsoft.

UPDATE RELIGIOUSLY The most important e-mail security tool is also your last line of defense: antivirus software that scans attachments before they're opened. To get the most from such software, religiously update the signatures, preferably by enabling any automatic update feature that the program provides. (Also make sure the e-mail component is turned on, as not all antivirus software has it switched on by default.) Outbound scanning--where the antivirus software probes attachments users send to guarantee they're not helping spread malware to others --may make them good citizens, but in a dog-eat-dog world, disable it to reduce the antivirus software's memory and/or processor appetite, and to speed up e-mail transmission.

Continue to the sidebar:

[Dig Out From The E-mail Crush](#)

Return to the story:

[Businesses Struggle Under Growing Weight Of E-mail](#)



[Copyright © 2003 CMP Media, LLC](#) | [Privacy Statement](#)