The Outlook Security Patch

Microsoft has introduced an Outlook security patch in response to the high-profile virus outbreaks earlier this year which used email to spread. We take a look at what it does and what its drawbacks are.

By PCNA Staff

Computer viruses are nothing new - the first PC virus was written more than 15 years ago. But whereas older viruses spread via executable files on floppy disks, modern ones spread via document files and Internet email. The enormous growth in use of the Internet has meant that new viruses such as the Love Bug, or ILOVEYOU, managed to hit literally millions of PCs in the initial wave before the virus scanner vendors managed to update their databases of known virus signatures.

ILOVEYOU, and Melissa before it, used Microsoft Outlook to spread. Melissa automatically looked up the first 50 names in the victim's Outlook address book and mailed a copy of itself to those people. The Love Bug mailed itself to every single person in the book. Because the resulting messages appeared to originate from a friend or colleague of the recipient, many recipients opened the message. After all, if a friend or colleague sent you a message with a header that possibly proclaimed their love for you, would you think for even a moment that simply clicking on the message to open it would start a virus running on your PC?

Needless to say, Microsoft came in for much criticism in the wake of virus outbreaks such as ILOVEYOU because of the ease with which the viruses could spread via Outlook. Clearly something had to be done. And so, at the end of June, Microsoft launched the Outlook Security Update. You'll find it on the Web at **www.officeupdate.com**, and it was also on last month's PCNA CD-ROM. The update is available for Outlook 98 and Outlook 2000, but not for Outlook Express. And the new Outlook Express 5.5, included with the Windows 2000 Service Pack 1 that you can order on CD from Microsoft, does not include the security update either.

The security update provides protection from most viruses that spread themselves through email, or worm viruses that can replicate through Outlook. The update works by limiting or removing certain functionality in Outlook. Thus, although it will stop many types of virus from spreading, it may also affect the legitimate function of other programs and also severely limit the facilities that users may be accustomed to using.

The Outlook 2000 patch requires that you first install Office 2000 Service Release 1a (not plain SR1). This can be found at **www.officeupdate.com** or, if you subscribe to our sister magazine PC Support Advisor, you'll find it on the CD-ROM. Be aware that the SR1a patch will require access to the original Office 2000 CD-ROM, or a copy of it on a server, so ensure that you have it handy.

Functionality

The Outlook update adds three new levels of security:

Email Attachments

Email attachment security permanently prevents users from accessing several file types when received as attachments. Affected file types include executables, batch files, and other file types that contain executable code often used by virus writers.

Object Model Guard

Object Model Guard prompts users with a dialog box when an external program attempts to access their Outlook address book or send email on their behalf, which is how viruses such as ILOVEYOU spread.

.EXE
.COM
.BAS
.VBS
.JS
.ISN
.LNK
.PIF

Figure 1 - Level 1 security files.

Revised Security Settings

The default security settings for Outlook have been changed, and increase the default Internet security zone setting within Outlook from "Internet" to "restricted sites". In addition, active scripting within restricted sites is disabled by default. See below for more on this.

Side Effects

The Outlook security update will affect certain functionality within Outlook, and may also have an impact on the interaction of some third-party software programs with Office.

Accessing Attachments

Once you install the update, users will not be able to access attachments with file types that could run executable code or change settings on a computer. These file types are known as Level 1 security files and they are listed in Figure 1. If a user receives a message that contains an attachment that cannot be accessed, the inbox will display the paperclip in the attachment column to let the user know that the message has an attachment. When the message is opened, the attachment will not be available.

On the File menu, the Save Attachments command and the View Attachments command on the shortcut menu will not be available for the message. In the case of a message with multiple attachments, the unsafe attachments will not be accessible but other attachments will be retained.

Save To Disk

If a user receives a message containing a Level 2 file as an attachment (see Figure 2 for details), he or she will be warned that the file must be saved to disk before it can be opened. It can't be executed directly from within Outlook.

Sending Attachments

When you attach a file to email, the update checks the file type when you send the message. If the file type is on the list of restricted files, you will be warned that other Outlook users may not be able to open the attachment. If you click Yes, the message is sent with the attachment. If other users have the update installed, the attachment will be inaccessible. If you click No, the message will be returned to you for editing, which will involve removal of the attachment.

Defaults

Default security zone settings are set to Restricted Sites (rather than Internet) by default, and active scripting within restricted sites is disabled by default when the patch is installed. The Restricted Sites security zone disables most automatic scripting and prevents ActiveX controls from opening without the user's permission. These security features help protect users from many viruses that are spread by means of scripting.

Conclusion

So, should you install the Outlook security patch? At face value, this seems like a daft question. Why would any company which uses Outlook not want to install such an important security update as this one? Unfortunately, it's not that easy. The patch has side effects which may have a big impact on the way that your users work, as it will permanently deprive them of the ability to receive executable attachments. Our advice is that, wherever possible, you should indeed install the patch, but think carefully before doing so.

PCNA

File types on the Level 2 security list must be saved to disk before they can be opened - the files cannot be opened directly from within Outlook. There are no file types on the Level 2 security list by default, but file types can be added to the list by system administrators.

Figure 2 - Level 2 security files.

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.