workshop

Index

Web security tips & tricks

Sneakier spam, wilier worms, more aggravating ads… It's no wonder that many of us sometimes feel as though our PCs are under assault. Dylan Tweney and Kim Zetter show you how to fight back with these simple steps for keeping the latest internet pests at bay

The latest viruses spread through everything from your instant messages to your file-sharing program. Annoying new ads hijack your browser without you even clicking them. Spam greeting cards send themselves to everyone in your address book. Next-generation auction swindles exploit what's supposed to be one of the safest ways to do business online.

As 2003 rolls on, the breakneck pace of new virus and worm development shows no signs of abating. Meanwhile, the most persistent and resilient nasties of 2002, such as Klez, still plague our inboxes.

But you can turn the tide against these pernicious pests. Here is *PC Advisor's* guide to the newest threats to your PC, from hackers to sneaky adware, and the tools you need to send them packing.

Ward off worms and viruses

Virus writers continue to find ever cleverer ways to deliver malicious code to our PCs, and with potentially devastating consequences. Email attachments remain the favourite approach but some worms target any widely used program that lets you download files, such as an instant messaging or file-sharing application.

ILLUSTRATION: AILEEN O'DONNELL

Can the spam

Most solutions for getting rid of spam recommend that you set up filters to block addresses that spam comes from, or delete messages that contain suspect words like 'viagra' or '$$$' in the subject line. If you follow these recommendations, though, spam still gets through – and you then waste even more time adding new filters to eliminate it.

A better method becomes obvious when you realise that spam is never addressed specifically to you. Unlike messages from friends, your email address doesn't appear in the To or CC header fields of unwanted emails. You may have friends who have discovered the BCC header field, which lets you send copies of messages to addresses that don't appear in the headers. Often, this is used to pass on chain letters, jokes and other material. You may be quite happy to treat these as spam.

If you want to receive these messages, however, create another intermediate rule that says 'Where the From line contains [friend's email address], stop processing more rules'.

Set up mail rules like this, and spam could cause you no more bother than a weekly check to empty your Spam folder.

1 Your first rule should say 'Where the To line contains [name] or where the CC line contains [name], stop processing more rules'. This will leave all mail specifically addressed to you in your inbox

2 The last rule should say 'For all messages, move it to the Spam bucket folder and mark it as read'. This lets you ignore unwanted messages. You can check the folder from time to time to see what the filter has caught. This will avoid you deleting an important message which got caught in the net

3 Some wanted emails may end up in the Spam folder – for example, subscribed mailing lists may not have your address in the To or CC headers. Create an intermediate rule, that stops filtering if the message is identified as coming from a mailing list, by checking for the list name in the subject line

Historically, viruses targeted only a single vulnerability such as a security hole in Internet Explorer or Outlook Express. The Slammer/Sapphire worm, for example, took advantage of a well-known security hole. A patch had been made available for it months earlier, but many hardware and software makers (including some at Microsoft) had not applied the fix.

It's no longer enough to install an antivirus program and personal firewall. Experts recommend you turn off Windows File Sharing (in the Networking Control Panel) if you don't need to use it and set your firewall to block file sharing on TCP ports 139 and 445.

Newer viruses are even more sophisticated. The infamous Klez worm relied on Outlook Express to reproduce and worms with built-in mail engines are the future direction of malicious code. Such variants spread independently of email programs and scout for victims anywhere on your hard drive, searching for addresses even in the web browser cache.

For hackers, the PC itself is often a more attractive target than its contents. And your infected machine can still be used to plunder your data, attack other PCs and wreak havoc on a network.

Some intruders use our PCs to dump potentially incriminating data. The hacker gains access to a number of computers and uses them to store illegal material such as pornography or stolen files.

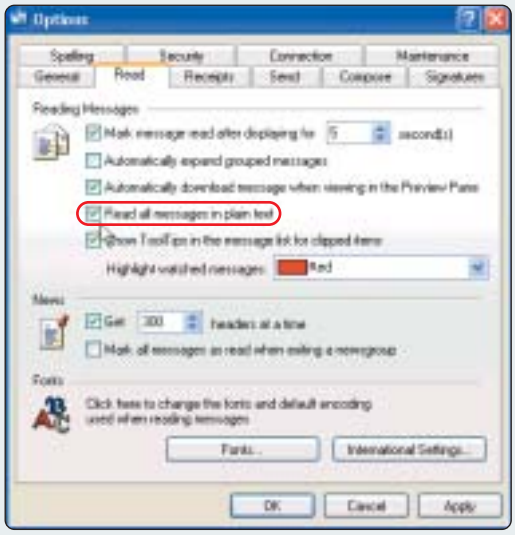
Operating from a PC free of damaging evidence, the hacker can view the files on the victim's machine at a convenient time and in relative safety. If the victim has a broadband connection and leaves the PC powered on day and night, all the better. Simply shutting off your PC when you're not using it is one of the easiest things you can do to avoid becoming a victim.

Even if your PC isn't online, the Lirva-based Avril Lavigne virus that was doing the rounds early this year will still cause havoc. All you have to do is preview the message in Outlook Express for it to disable your antivirus software, dial your ISP and spread itself like bindweed via email, instant messenging and file-sharing networks such as Kazaa. Those affected by this Trojan should download the Lirva Removal Tool at http://securityresponse.symantec.com/avcenter/venc/data/w32.lirva.removal.tool.html.

Worms like Lirva have the ability to spy on infected PCs and alter stored data. Music download fans should be

Protect yourself with plain text

Worm viruses, which can be activated simply by viewing a message in Outlook Express' preview pane, can cause havoc if your copy of Outlook Express isn't bang up to date and you don't have a good viruschecker. Even if those security measures are in place, some users are still understandably wary of formatted emails. The answer is to read your emails in plain text as there's no way to conceal a virus in a plain text message.



To enable the plain text option in Outlook Express, click Tools, Options and select the Read tab. Under 'Reading messages' check the box entitled 'Read all messages in plain text'.

particularly wary of such file-sharing apps. While you let them happily download those must-have tunes, vulnerabilities in Kazaa's pop-up ads, for example, could let malicious code gain control over your PC.

More than just junk

Spammers are also inventing new ad delivery techniques that grab more and more control of your web browser. The newest, most insidious type of pop-up ad doesn't even require you to click on it to take you to another site. Simply moving your pointer over the ad in a certain way will send your browser to an advertiser's web page.

Advertisers call these 'kick-through' ads, a more aggressive spin on the term click-through (defined as when you deliberately click an ad and visit the advertiser's site).

A few advertising companies now produce software that attempts to download a browser plug-in or program to your system when you visit a page with their ads on it. The plug-in monitors where you surf and places relevant ads in front of the browser window.

Other companies use freeware internet tools such as bandwidth speed testers that appear to load adware on to your PC, change your browser's home page and settings and monitor what you do online. Beware: some purport to be search tools while others claim to speed up downloads or, unbelievably, block pop-up ads.

PC users can fight back against intrusive advertising by using ad-blocking software such as AdSubtract (www.adsubtract.com). Set your hardware firewall to block internet domains advertisers use, such as Doubleclick.net and Advertising.com. Over time, as you add new advertiser domains to the firewall's exclusion (or blocked domain) list, you'll be pestered by fewer ads.

The Google Toolbar (http://toolbar.google.com) also has an option that blocks one common technique advertisers use to spawn more pop-up ads when you close a web page.

Marketers push advertisements through Windows' Messenger service (an admin feature in 2000 and XP systems that spawns a pop-up similar in appearance to a dialog box, whether your browser is open or not). The ads can pop up anytime you're connected to the internet, even if you're simply writing a Word document. Block them by turning off the Messenger service or installing a firewall.

Antispam tools such as SpamKiller (www.mcafee.com) promise to filter nearly all unwanted commercial emails from your inbox. Some ISPs tout the spam filtering on their email systems while services like ChoiceMail One (www.digiportal.com) let you set lists of people who are forbidden to send you mail.

Protect your platform

Of course, faced with all these insecurities and modes of attack it helps to stem the problem from both ends. So make sure your operating system is as secure as it can be and patch any potential holes.

• **Windows XP** Both XP Home and Professional users have security problems stemming from Universal Plug and Play. These include glitches in the way XP handles SSL certificates from secure websites and a bug that could prevent you accessing encrypted files after you change your password.

Install Windows XP Service Pack 1 from www.microsoft.com/windowsxp/pro/downloads/servicepacks/sp1/default.asp. Right-click My Computer, select Properties and choose the Automatic Updates tab. Tick the box beside 'Keep my computer up to date' and specify whether you want Auto Update to tell you before it installs updates or if you want it done automatically.

Patches can cause difficulties if released before being thoroughly tested, so set Windows to notify you before it installs anything. If the reminders irritate you, turn off Auto Update but don't forget to check periodically for new patches.

• **Windows Me** This OS has a number of security holes, including the way it handles digital certificates and a bug that lets unauthorised network users view shared folders on your PC. There's no service pack nor a single list of patches so your best bet is to go to the Windows Update site at http://v4.windowsupdate.microsoft.com/en/default.asp.

• **Windows 2000** This version has hundreds of security holes and bugs, including multiple flaws relating to password theft and denial-of-service attacks. Service Pack 3 (get it from www.microsoft.com/windows2000/downloads/servicepacks/sp3/default.asp), which also includes XP's Automatic Update feature, will help fend them off.

The Windows 2000 High Encryption Pack at www.microsoft.com/windows2000/downloads/recommended/

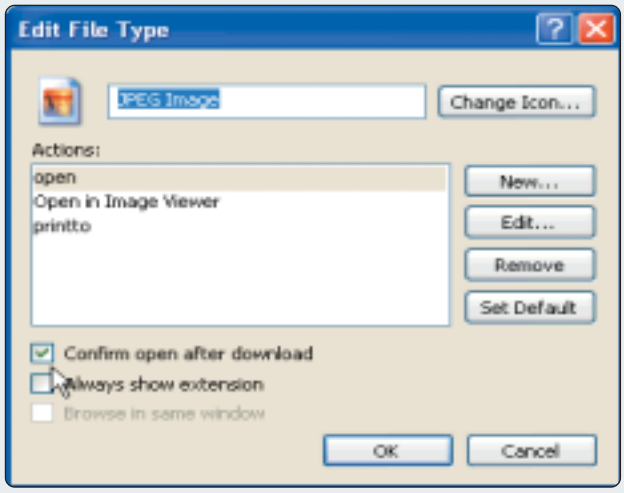
Be choosy about your attachments

If you use a good, up-to-date viruschecker that provides on-access virus scanning you can let it take care of deciding whether an attachment is really dangerous or not. However, if you like the belt-and-braces approach you can enable the 'Do not allow attachments to be saved or opened that could potentially be a virus' setting under the Security tab of Outlook Express' Options and simply configure it so that only attachments that really are potentially dangerous are blocked.

Also check that the 'Confirm open after download' option is selected for the file types that are commonly used to spread viruses such as HTA, JS, JSE, VBE, VBS, WSF, WSH and DOT. Other file types that can spread viruses include BAT, CMD, COM, EXE and PIF.

Windows XP won't let you see the settings for these system files. If you use this operating system then you can assume that they are already correctly set.

1 Click on Tools, Options and select the Security tab, you'll see an option that says 'Do not allow attachments to be saved or opened that could potentially be a virus'. If this box is ticked, when Outlook looks at its checklist of potentially dangerous attachments, some harmless attachments are flagged as possible viruses and, as a result, Outlook won't allow you to open them or save them to your hard disk



2 In order to see those safe attachments, open Folder Options from Control Panel or Windows Explorer and select the File Types tab. Scroll down the list to locate the file type that Outlook Express is blocking – for example, Jpeg files – select it and click the Advanced button. On the Edit File Type window you'll see an option that says 'Confirm open after download'. This is the setting that Outlook Express uses to determine whether a file type is potentially dangerous or not. If you clear this checkbox and click ok then Outlook Express will no longer block access to files of this type

encryption provides 128bit encryption support for websites that run on a Windows 2000 server, increasing the security of online transactions.

• Windows 98 The Customer Service Pack at www.microsoft.com/windows98/downloads/default.asp fixes login and password flaws along with a few stability issues. Windows 98 SE users don't need this service pack. Additional security updates for Windows 98 and 98 SE correct weaknesses that allow hackers to run malicious code on your PC. Go to www.microsoft.com/windows98/downloads/corporate.asp for a full list of updates, links and patches.

Spot scammers and thieves

Big auction sites claim they aggressively fight cyberfraud, in part by promoting the use of escrow services which act as honest middlemen in an online transaction. They hold a buyer's money until goods arrive and then transfer the funds to the seller. But fake escrow sites cheat auction buyers and sellers (though not in the same transaction) and make off with both money and goods.

More than a hundred scam escrow sites have popped up in the last year, many of them chronicled at www.sos4auctions.com. The site offers clues for spotting the fakes and tips on how to get the most out of a good, established service.

It always pays to check the background of an escrow site you're not familiar with at SOS4Auctions or the Better Business Bureau (www.bbbonline.org) before you commit to any purchase. If the escrow service lists a mailing address and telephone number, ask the BBB to consult its records to see whether anyone has filed complaints against the company. ■

Find out where to get patches for popular email, browser and instant messenger software online www.pcadvisor.co.uk/printplus