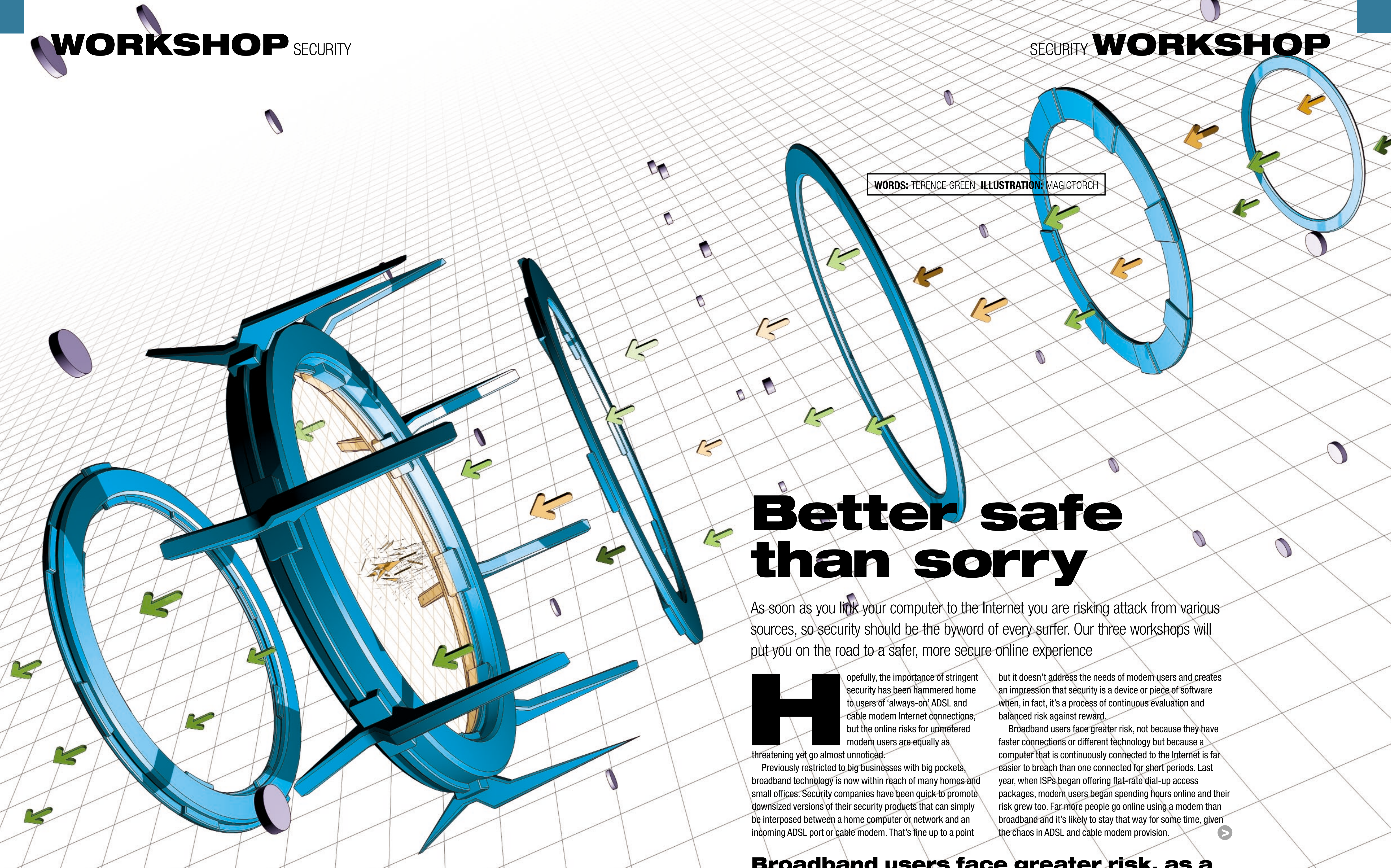


WORDS: TERENCE GREEN **ILLUSTRATION:** MAGICTORCH

Better safe than sorry

As soon as you link your computer to the Internet you are risking attack from various sources, so security should be the byword of every surfer. Our three workshops will put you on the road to a safer, more secure online experience

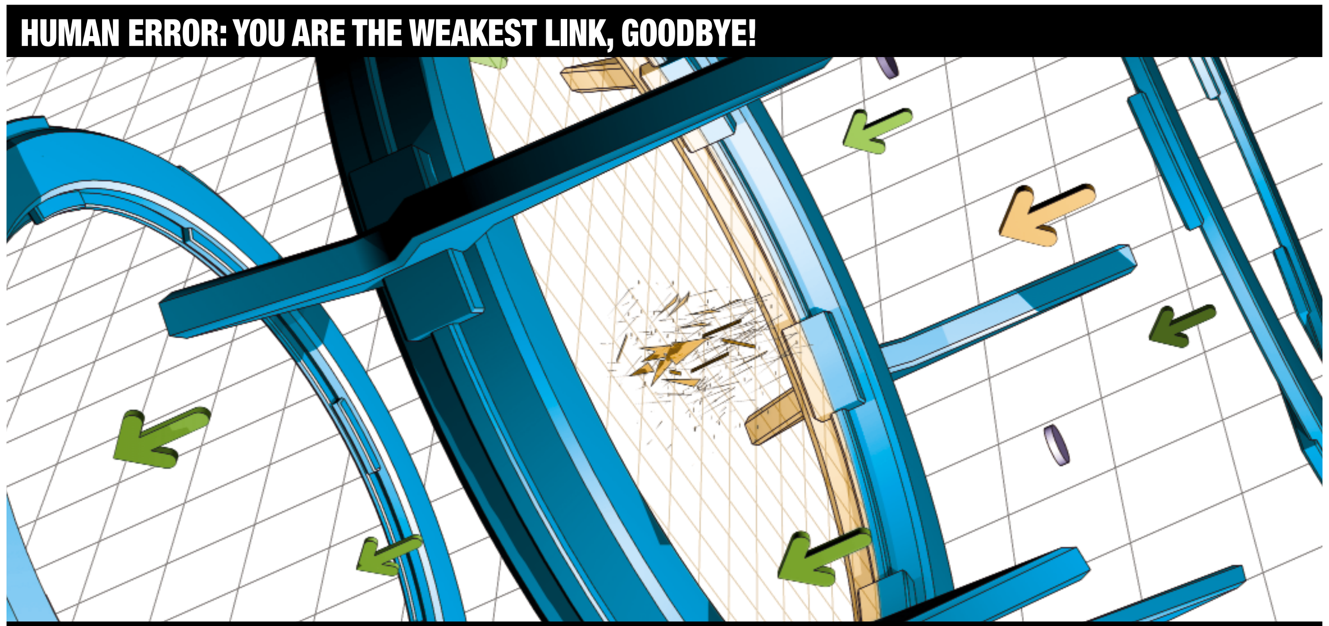
Hopefully, the importance of stringent security has been hammered home to users of 'always-on' ADSL and cable modem Internet connections, but the online risks for unmetered modem users are equally as threatening yet go almost unnoticed.

Previously restricted to big businesses with big pockets, broadband technology is now within reach of many homes and small offices. Security companies have been quick to promote downsized versions of their security products that can simply be interposed between a home computer or network and an incoming ADSL port or cable modem. That's fine up to a point but it doesn't address the needs of modem users and creates an impression that security is a device or piece of software when, in fact, it's a process of continuous evaluation and balanced risk against reward.

Broadband users face greater risk, not because they have faster connections or different technology but because a computer that is continuously connected to the Internet is far easier to breach than one connected for short periods. Last year, when ISPs began offering flat-rate dial-up access packages, modem users began spending hours online and their risk grew too. Far more people go online using a modem than broadband and it's likely to stay that way for some time, given the chaos in ADSL and cable modem provision.

Broadband users face greater risk, as a computer that is continuously connected to the Internet is far easier to breach

HUMAN ERROR: YOU ARE THE WEAKEST LINK, GOODBYE!



As far as security is concerned, humans are the weakest link. In terms of risk, human error is often perceived to involve action – opening attachments, downloading from dodgy websites – by the user, but that's not always so. In the March issue, we carried a workshop on making Outlook Express less of a security loophole. Shortly afterwards a reader contacted us to say that, despite having followed our instructions to the letter, Outlook Express was still initiating an automatic dial-up networking (DUN) connection on receipt of a particular email.

This is the result of a 'good idea' designed to liven up email that has the unexpected side effect of creating a security risk. Email clients such as Outlook, Outlook Express and Netscape Messenger use the Internet Explorer HTML viewer embedded in Windows to display font and image effects when HTML codes are embedded in the incoming email message. At present, this action cannot be disabled in Outlook or Outlook Express, even if all scripting is disabled, and it can be exploited by malicious code in HTML mail. Fortunately, our reader's problem involved references to benign images stored on a website. The DUN connection was triggered when Outlook Express attempted to retrieve them. Microsoft's desire to enhance the email experience removes the responsibility for human error from the only person in a position to make a judgement call at the point of impact.

Human error should never be discounted, but that happens often. Microsoft's security framework is predicated on digitally signed code. A digital certificate such as the one you see when using Windows Update certifies that the code you downloaded originated from Microsoft. Accept it and the code runs completely unrestricted on your system.

Recently, Verisign, the leading issuer of security certificates, sold some digital certificates to someone posing as Microsoft. Whoever obtained these certificates under false pretences could disseminate software certified as coming from Microsoft that trashed your hard disk or worse. Once Microsoft realised how serious this act was it posted a Critical Update. If you install it you shouldn't have to worry about the two spurious certificates any more, but Verisign's error is a salutary lesson on how the responsibility for trust can be blurred.

The security warning displayed when Explorer encounters a digital certificate doesn't verify the code, it verifies the publisher that asserts its code is safe. That assertion is as trustworthy as the publisher. Someone posing as Microsoft has done us all a favour by demonstrating that, in reality, it is our responsibility to trust all incoming code.

According to research published in February by Oftel, the UK Government regulator for telecommunications, 2.3 million UK homes had some form of unmetered access by the end of 2000. At that time the total number of unmetered broadband services (ADSL and cable modems) was under 50,000; since Home Highway (ISDN) is a minority sport, it's safe to say that over two million homes in the UK have unmetered modem connections to the Internet.

Two million homes connected to the Internet for hours at a time is a big target for anyone with mischief in mind. If our mischievous friends also have unmetered access they have all the time they need to test our defences. This, of course, assumes a risk in the first place. It's not uncommon to believe that talk of security problems, such as anti-virus scares, is no more than a sales pitch designed to encumber the unwary with costly or unnecessary security devices. Would that it were so! The fact is, when you connect your computer to the Internet you're also, naturally, connecting the Internet to your computer. You can discount this as a risk only if you believe there are no bad guys out there. Many of the bad guys are just amateurs playing with tools they barely understand, but they can still cause problems, as demonstrated recently by the Kournikova virus. Clearly, when we use the Internet, we have to accept that there are risks. We can ignore them and surf regardless, we can avoid all risk by not connecting to the Internet at all, or we can compromise and minimise risk without restricting our use and enjoyment of the Internet.

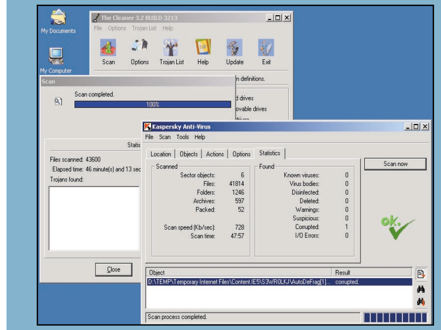
Security is the process of arriving at that compromise and it should be a continuing process since risk changes, often as a result of our own behaviour. An email attachment is a risk; opening it magnifies the risk. We can also influence the nature of the risk. Many unsolicited emails (spam) include an 'unsubscribe' option. By itself, the spam may present a slight risk but responding with a request for your name to be removed from the list will validate your email address for the spammer and open you up to a new set of risks.

Realising that we are part of the problem is essential to defeating the biggest security flaw of all – the belief that security is something we can interpose between us and the bad guys. In reality, security is what we trust and, as the *Human error* box (left) shows, all we can really trust is what we can touch, and even that's suspect. This isn't a counsel of despair, only a reminder that installing a piece of software or hardware is only part of the security process.

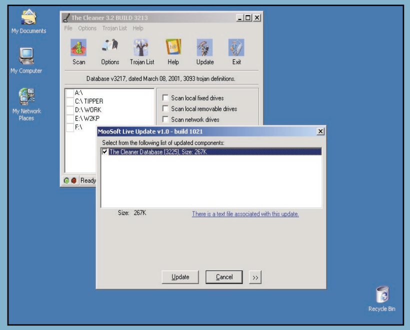
To create effective security we need an awareness of the type of risks we face. When we first consider risk it's natural to assume that threats arrive from outside and are aimed at us, but it works both ways. We need to protect our data against external threats but, increasingly, our data is an unfortunate bystander as high-profile attacks have demonstrated. Classic examples such as the I Love You and Melissa viruses take swipes at our data, but are far more effective at propagating themselves via the Windows address book to all our contacts.

As many can attest, by far the biggest threat to our data is an operating system or software/hardware glitch, or simple human error. We install a new peripheral, something goes wrong, and suddenly we're reinstalling the operating system. The only way to recreate our data is by restoring from a recent backup; this also happens to be an essential security tool should some incoming threat wreak havoc on your data. To cover for the situation where you don't spot a problem immediately, use a grandfather-father-son backup strategy

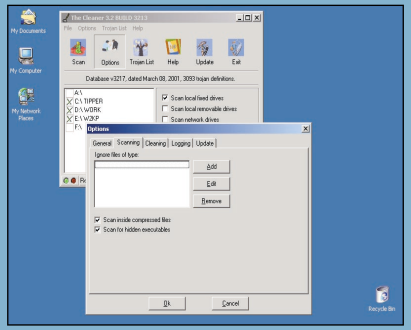
HOW TO CHECK FOR VIRUSES AND MALICIOUS CODE



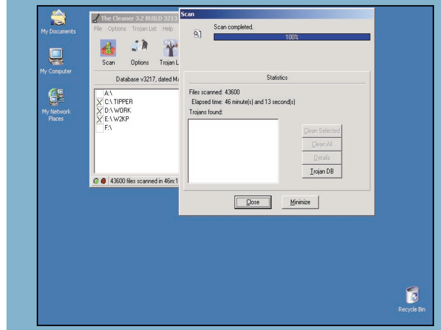
1 Before securing your system, ensure it isn't already harbouring any nastiness like trojans and backdoors. You have several options; The Cleaner (www.moosoft.com) is a trojan-specific scanner and cleaner available on a 30-day trial. Since you should also scan for viruses, which The Cleaner doesn't do, you may prefer to use a quality anti-virus scanner, such as KAV from www.kaspersky.com, which has a good reputation for detecting trojans and viruses. Or use both to be double certain.



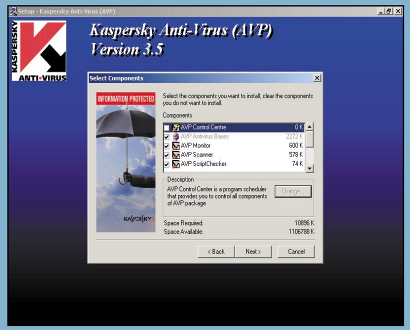
2 Download and install The Cleaner from www.moosoft.com. Start it and click on the Evaluate button. This is a fully functional version. The database loads and the scanner window is displayed, but to get the best results, connect to the Internet and update the database so that you are using the latest trojan definitions when you scan your drives. Click on the Update button and follow the prompts to download and install the most recent database.



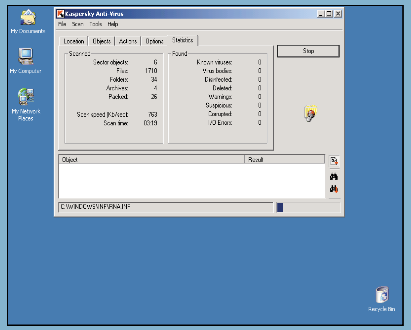
3 In The Cleaner window next to the list of drives, click on 'Scan Local Fixed Drives' to select them. Since we want to perform a comprehensive scan, click on the Options button and on the Scanning tab and select both Scan inside compressed files and Scan for hidden executables. The scan will take longer but will now detect trojans that use stealth techniques to hide themselves, as well as any that may be hiding inside file archives.



4 Close the Options windows and click on the Scan button to initiate the scan. Depending on the speed of your processor and the amount of data storage you have, this could take quite a long time because of the depth of the scan. If any trojans are discovered, click on the Clean All button to remove them. Use the Details button for more information or the TrojanDB for some interesting descriptions.



5 Go to www.kaspersky.co.uk to download a copy of Kaspersky Anti-Virus (AVP) Gold. Request a 30-day trial when offered as this enables full function which you need in order to download the latest anti-virus signatures. Install KAV using the Custom option to deselect AVP Control Centre as this is only required for centralised administration on networks. Reboot as requested once installation has completed and select OK to download updates from the Internet when prompted.

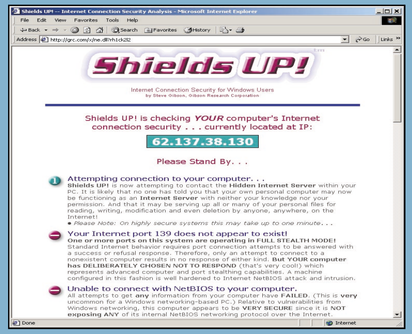


6 Start the Kaspersky AVP Scanner from the Programs menu. Select Local hard disks from the Location menu, from the Objects menu select all the objects and set file type to All, leave the remaining options unchanged, and click on Scan. Since every file as well as compressed files and mail databases will be checked, this will also take some considerable time. If any viruses are found, read the Help file and then disinfect them.

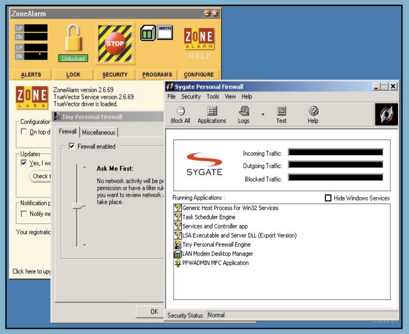
QUICK TIP

Never ever 'fit-and-forget' anti-virus software or personal firewalls. Update anti-virus signatures at least once a week – more frequently if you're using an unmetered connection – and check for program updates regularly.

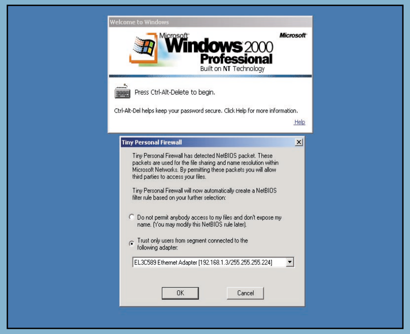
HOW TO INSTALL A PERSONAL FIREWALL



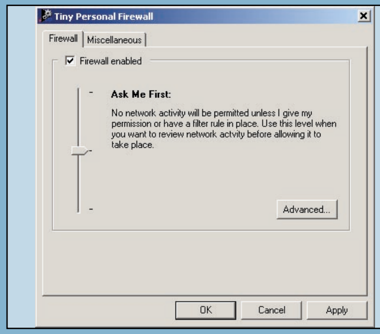
1 Several personal firewalls are free for home use, including Sygate Personal from www.sygate.com, Tiny Personal Firewall from www.tinysoftware.com and Zone Alarm from www.zonelabs.com. Try them all to see which fits your needs. After installing your firewall, visit http://grc.com and use ShieldsUp and LeakTest to see how well it performs. As a Windows user you want to be sure that NetBIOS isn't being exposed through your Internet connection.



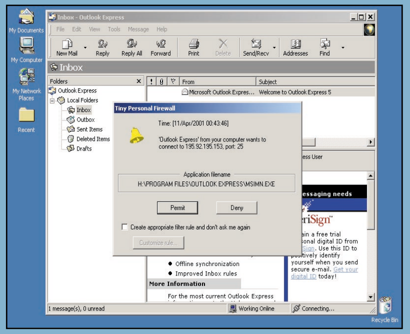
2 Personal firewalls aren't toys; they do a good job of closing obvious holes in Windows and can prevent trojans that have managed to install themselves on your system from making outbound connections, but you shouldn't depend on a free software firewall if you have truly sensitive data to protect. Zone Alarm is the easiest to use because it is highly automated, but Tiny and Sygate are more flexible if you want to learn more about how personal firewalls work.



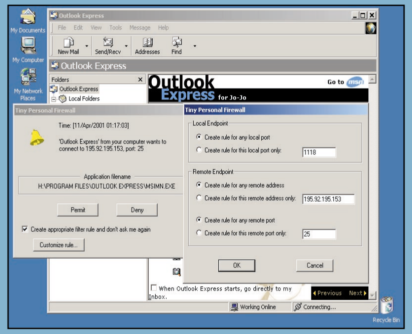
3 Tiny Personal Firewall most resembles a traditional firewall. Installation takes minutes, then you must reboot so Tiny can load itself before any other application that might access the Internet. If you have a network card installed, Tiny will detect it and let you choose whether you allow other computers on the same local network to access Windows resources on your computer. Tiny will create a rule based on your reply.



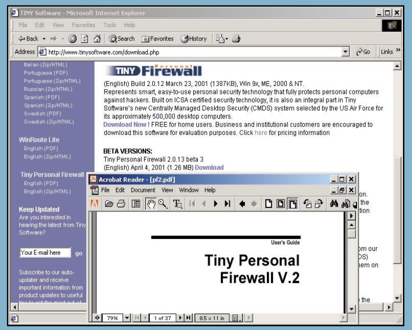
4 Tiny (and ZoneAlarm and Sygate) are intrusive at first because they default to blocking all communication between your computer and the Internet. Open Tiny's Personal Firewall Administration window from the System Tray icon or the Start menu. The default option 'Ask Me First' ensures that no network/Internet traffic will be passed without your say-so. A dialog box will pop up the first time an app attempts to transmit to or is contacted from the Internet.



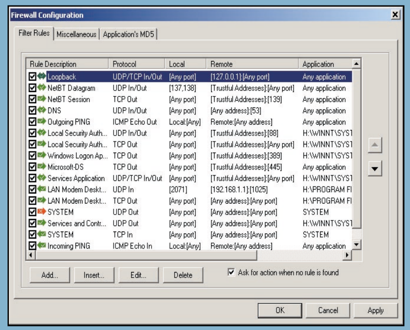
5 To be notified every time there is communication between an app and the Internet, click on 'Permit' or 'Deny' to allow the current action. Manual Permit/Deny options are normally only used when you are familiar with an app but don't know why it needs to communicate with the Internet. If you Deny access and the app doesn't malfunction you can set a Deny rule next time; if it does malfunction with Deny you have to consider setting a 'Permit' rule.



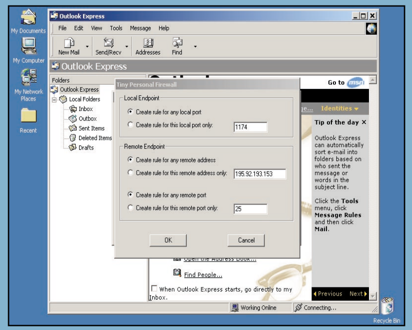
6 Initially, rules are created in order to automate those processes you decide to allow. They can be refined later. Place a tick in the box next to 'Create a filter rule...' and click on Permit or Deny to create a rule for outgoing and/or incoming communication whenever this particular set of circumstances occurs in future. To place further restrictions on the rule click on the 'Customise rule' button before confirming the rule with the 'Permit' or 'Deny' buttons.



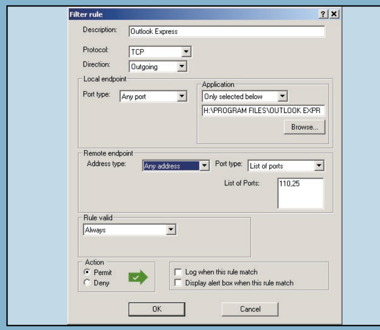
7 As Tiny Personal Firewall does not include any Help, you may wish to download the User's Guide from the Tiny Software website. It is a little out of date but offers some help on the custom settings. Normally, the default settings are satisfactory, but as you learn more about firewalls and how your applications interact with them you may want to limit some outgoing actions to specific remote ports in order to tighten up security.



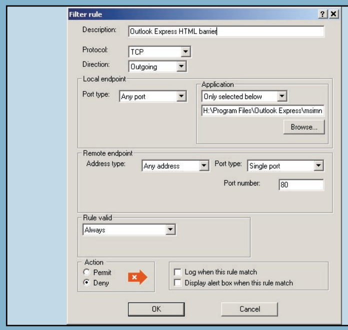
8 Rules can be edited or deleted at any time. You should delete rules for apps you no longer use. Open the Personal Firewall Administration window on the Firewall tab and click on the Advanced button to display the rules. The first rule, the Loopback, is mandatory. If you remove it the firewall won't be able to communicate with the operating system and you will need to reinstall the firewall to re-establish the Loopback rule.



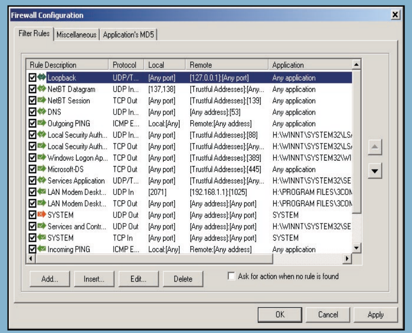
9 As you become familiar with the firewall you can begin to refine the rules. If you use Outlook Express, use Administration to delete its rule. Run Outlook Express send/receive and opt to customise the rule. Restrict the remote address and port the specific numbers listed. When you next try to send and receive Outlook Express will only be able to send mail because the rule does not include port 110, the port for receiving mail. The rule is too restrictive.



10 To create a specific Outlook Express rule go to Filter Rules and Edit its rule. Change port to 'List' and add 25 (SMTP send) and 110 (POP3 receive). Leave the remote endpoint address at 'Any Address' if you collect mail from multiple mail servers. With this rule in place Outlook Express can send and receive mail but won't be able to access newsgroups. Our rule is becoming very complicated, and we're not making Outlook Express any safer.



11 To make Outlook Express less of a risk we must stop it opening web URLs in response to emails containing potentially risky HTML code. One way of doing this would be to return to the original general rule for Outlook Express and to insert a new rule above it that denies it access to port 80, the port used by web servers. If the web filter rule came after a general rule allowing all access it would have no effect.



12 Constructing rules is a tricky business but you can find plenty of help on the web and in newsgroups for whichever personal firewall you settle on. At any time you can return to the starting point by deleting the rules you have created. Once you have finalised your ruleset you can disable 'Ask for action when no rule is found' and any action you haven't explicitly permitted will be denied. For a correctly configured firewall this is the safest option.

QUICK TIP

Use Windows Update to install critical updates on a regular basis, and don't be deterred by large time-consuming downloads. Be especially vigilant if Internet Explorer is installed and you use Outlook or Outlook Express.

to keep at least three weekly generations of full backups. Periodically, take a full backup out of the cycle and store (archive) it off-site as a precaution against flood, fire or meteors taking out your entire home.

The risk of inconveniencing friends and alienating business contacts by spreading a virus such as I Love You to them through the Windows address book is one we can all understand, but most incoming attacks these days carry multiple warheads. I Love You is classified as a worm because it propagates itself via email over a network. This has the side effect of overloading some mail servers and causing them to shut down. I Love You also contains a component (a trojan) that surreptitiously attempts to connect to a website to download a program that steals passwords.

Other recent attacks such as Kournikova have also attempted to connect to websites for various reasons. If many connection attempts all happen in a short space of time, as would happen when a virus spreads rapidly, they can overload web servers or the routers that control Internet traffic. Some attacks, called Denial of Service (DoS) attacks, are specifically designed to do just this, preventing Internet sites from providing service. Under certain circumstances an attacker could co-ordinate multiple computers to mount a Distributed Denial of Service (DDoS) attack. A year ago, many major websites, including Yahoo, MSN and Amazon, were overwhelmed by a flood of incoming traffic that cut them off from the web. Dozens of Internet servers became the unwitting accomplices of the perpetrators.

Although there is no evidence yet of a co-ordinated DDoS attack using home computers, there are many different ways in which a DDoS attack could be mounted, several known DoS programs, and plenty of ways in which they can be distributed to large numbers of computers.

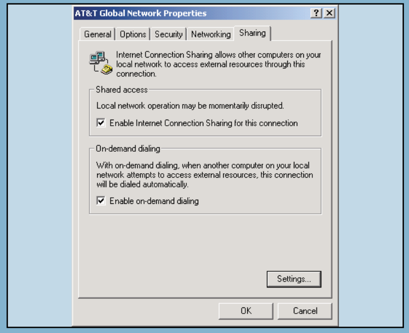
On top of this, a whole class of programs called 'backdoors', the best known of which are BackOrifice and Subseven, can use file attachments or web downloads to secretly install a remote access client on your computer. The client will broadcast its presence whenever you are online and allow anyone who picks up the call to control your computer remotely. Depending on the capabilities of the remote client your computer could be used to mount an attack on another computer, or something equally as sinister, while you're innocently browsing the web.

With many more people spending ever longer online thanks to unmetered access and almost exclusively using Windows, an operating system with numerous security loopholes that most users aren't aware of and therefore don't fix, the risk of mischief is high. Enlightened self-interest says

QUICK TIP

Raise your awareness of security issues and receive rapid notification of new threats by signing up to receive regular newsletters on the latest security issues from a security advisory site such as www.securityportal.com.

HOW TO TIGHTEN UP LOCAL SECURITY FOR A HOME NETWORK



AT&T Global Network Properties

Internet Connection Sharing allows other computers on your local network to access external resources through this connection.

Shared access

Local network operation may be momentarily disrupted.

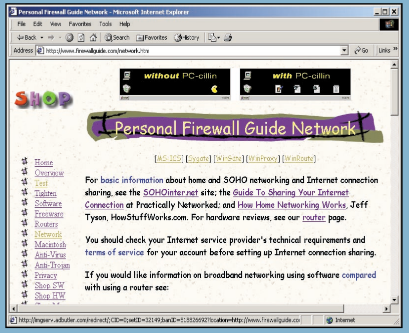
☑ Enable Internet Connection Sharing for this connection

On-demand dialing

With on-demand dialing, when another computer on your local network attempts to access external resources, this connection will be dialed automatically.

☑ Enable on-demand dialing

1 Many homes run two or more computers connected to the Internet through a dial-up connection by means of a proxy such as Windows Internet Connection Sharing (ICS). Proxies are similar to firewalls in that they inspect data transmissions and decide how they are treated, but a proxy doesn't necessarily replace a firewall. For a free firewall/proxy combo, use ICS and install the Sygate or Tiny personal firewall on all computers that connect to the Internet.



Personal Firewall Guide Network - Microsoft Internet Explorer

Address: http://www.firewallguide.com/network.htm

Personal Firewall Guide Network

[MS-ICS] [Sygate] [WinGate] [WinProxy] [WinRoute]

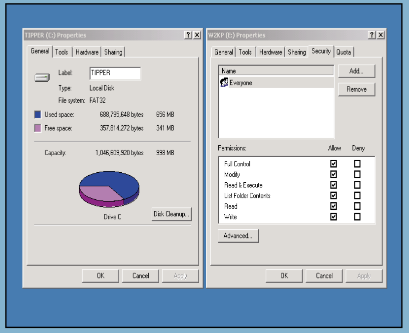
For basic information about home and SOHO networking and Internet connection sharing, see the SOHOinter.net site; the Guide To Sharing Your Internet Connection at Practically Networked; and How Home Networking Works, Jeff Tyson, HowStuffWorks.com. For hardware reviews, see our router page.

You should check your Internet service provider's technical requirements and terms of service for your account before setting up Internet connection sharing.

If you would like information on broadband networking using software compared with using a router see:

http://imgserv.adbutler.com/redirect/;CID=0;setID=32149;banID=518826692?location=http://www.firewallguide.co

2 A personal firewall only protects the computer on which it is installed and the firewall installed on the computer that shares its Internet connection (the gateway) must be capable of working with the proxy. Tiny also sells firewall/proxy packages. You can find more information about connection options for home networks at www.firewallguide.com.



TIPPER (C:) Properties

Label: TIPPER

Type: Local Disk

File system: FAT32

Used space: 688,795,648 bytes 656 MB

Free space: 357,814,272 bytes 341 MB

Capacity: 1,046,609,920 bytes 998 MB

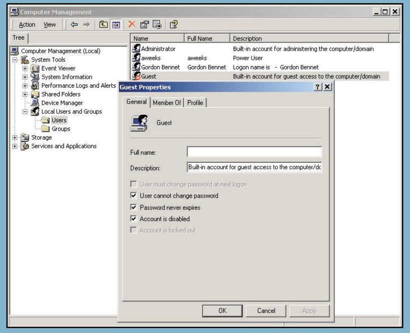
Drive C

W2KP (E:) Properties

Name: Everyone

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

3 If you're planning to share a modem connection to give a home network access to the Internet, consider upgrading the gateway computer to Windows 2000 Professional to provide an additional layer of security that Windows 98 and Me cannot. Security permissions that prevent outsiders from accessing sensitive data can be applied to hard disks formatted with Windows 2000's NTFS file system, which also allows files to be encrypted.



Computer Management

Name	Full Name	Description
Administrator		Built-in account for administering the computer/domain
aweeks	aweeks	Power User
Gordon Bennet	Gordon Bennet	Logon name is - Gordon Bennet
Guest		Built-in account for guest access to the computer/domain

Guest Properties

Guest

Full name:

Description: Built-in account for guest access to the computer/dc

□ User must change password at next logon

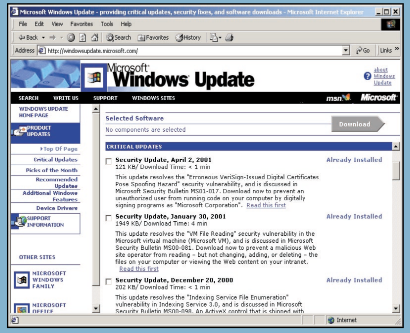
☑ User cannot change password

☑ Password never expires

☑ Account is disabled

□ Account is locked out

4 In order to use Windows 2000 security permissions effectively, do not enable the Guest account as this will allow anyone inside or outside the network to gain anonymous access to Windows 2000. Each person who will use the shared Internet connection should be given a User account on the Windows 2000 system. They will only be given access to Windows 2000 if they log on to their computer with their Windows 2000 username and password.



Microsoft Windows Update - providing critical updates, security fixes, and software downloads - Microsoft Internet Explorer

Address: http://windowsupdate.microsoft.com/

Microsoft Windows Update

Selected Software

No components are selected

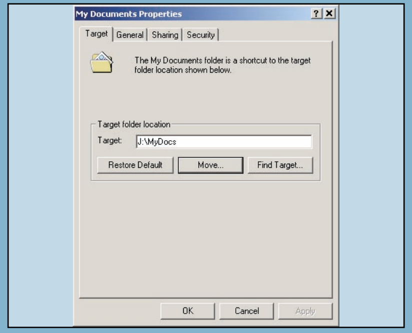
CRITICAL UPDATES

□ Security Update, April 2, 2001 — Already Installed
121 KB/ Download Time: < 1 min
This update resolves the "Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard" security vulnerability, and is discussed in Microsoft Security Bulletin MS01-017. Download now to prevent an unauthorized user from running code on your computer by digitally signing programs as "Microsoft Corporation". Read this first

□ Security Update, January 30, 2001 — Already Installed
1949 KB/ Download Time: 4 min
This update resolves the "VM File Reading" security vulnerability in the Microsoft virtual machine (Microsoft VM), and is discussed in Microsoft Security Bulletin MS00-081. Download now to prevent a malicious Web site operator from reading – but not changing, adding, or deleting – the files on your computer or viewing the Web content on your intranet. Read this first

□ Security Update, December 20, 2000 — Already Installed
202 KB/ Download Time: < 1 min
This update resolves the "Indexing Service File Enumeration" vulnerability in Indexing Service 3.0, and is discussed in Microsoft Security Bulletin MS00-098. An ActiveX control that is shipped with

5 Whichever version of Windows you use, and whether on standalone or networked computers, upgrade Internet Explorer to version 5.01 Service Pack 2 or later as earlier versions had security weaknesses that affect Outlook Express and other apps that use the Internet Explorer services embedded in Windows. Install ALL critical security updates. Use Microsoft Downloads rather than Windows Update if you wish to download updates once for several computers.



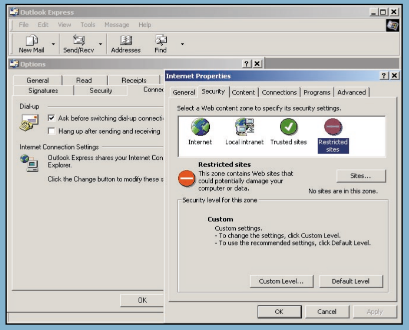
My Documents Properties

The My Documents folder is a shortcut to the target folder location shown below.

Target folder location

Target: J:\MyDocs

6 When installing applications or using Windows locations such as 'My Documents', specify a custom location rather than the default for storing data files. This will make it harder for someone who gains access to your computer to locate your data and it will be easier to set up data backups. If you create your own recovery CDs, hard disks divided into C: drives for systems and apps and D: drives for data will speed up recovery after a system crash.



Outlook Express — Options

Dial-up

☑ Ask before switching dial-up connecti

□ Hang up after sending and receiving

Internet Connection Settings

Outlook Express shares your Internet Con Explorer.

Click the Change button to modify these s

Internet Properties

Select a Web content zone to specify its security settings.

Restricted sites

This zone contains Web sites that could potentially damage your computer or data.

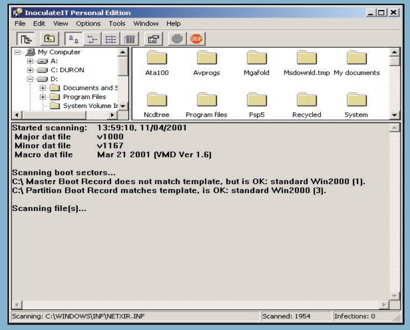
No sites are in this zone.

Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

7 If you must use Outlook Express, use Tools/Options/Security to move it into the Restricted Zone; then click on the Connections tab and use the Change button to open Internet Properties. Click on Security, click on Restricted Sites, click on Custom level, and make sure all settings are at 'Disable', 'Prompt' or 'High Safety'. Scripting should be disabled. Consider using less insecure email and news clients such as Forte Agent (www.forteinc.com), Pegasus, Eudora and PocoMail.



InoculateIT Personal Edition

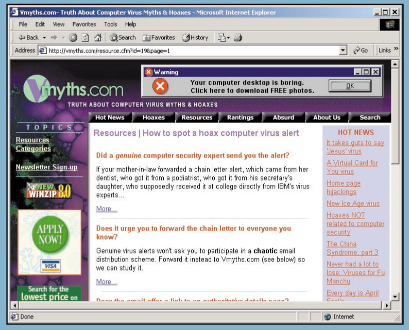
```
Started scanning:   13:59:10, 11/04/2001
 Major dat file     v1000
 Minor dat file     v1167
 Macro dat file     Mar 21 2001 (VMD Ver 1.6)

Scanning boot sectors...
C:\ Master Boot Record does not match template, but is OK: standard Win2000 (1).
C:\ Partition Boot Record matches template, is OK: standard Win2000 (3).

Scanning file(s)...
```

Scanning: C:\WINDOWS\INF\NETXIR.INF   Scanned: 1954   Infections: 0

8 Use a top-quality anti-virus (AV) program with its on-access monitor enabled on your gateway computer to ensure that all incoming data is scanned. Update signatures regularly. Install AV software on each networked computer. A free scanner such as Inoculate (http://antivirus.cai.com) saves splashing out on network licence fees. Set email clients to save attachments to a single folder and scan daily. You can't do this with Outlook Express as it saves mail and attachments in a single database.



Vmyths.com- Truth About Computer Virus Myths & Hoaxes - Microsoft Internet Explorer

Address: http://vmyths.com/resource.cfm?id=19&page=1

Warning: Your computer desktop is boring. Click here to download FREE photos.

Resources | How to spot a hoax computer virus alert

Did a *genuine* computer security expert send you the alert?

If your mother-in-law forwarded a chain letter alert, which came from her dentist, who got it from a podiatrist, who got it from his secretary's daughter, who supposedly received it at college directly from IBM's virus experts...

More...

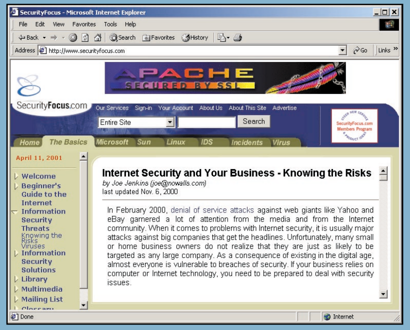
Does it urge you to forward the chain letter to everyone you know?

Genuine virus alerts won't ask you to participate in a **chaotic** email distribution scheme. Forward it instead to Vmyths.com (see below) so we can study it.

More...

Vmyths.com
TRUTH ABOUT COMPUTER VIRUS MYTHS & HOAXES
OK
Hot News
Hoaxes
Resources
Rantings
Absurd
About Us
Search
TOPICS
Resources Categories
Newsletter Sign-up
NEW WINZIP 8.0
APPLY NOW!
VISA
Search for the lowest price on
HOT NEWS
It takes guts to say 'Jesus' virus
A Virtual Card for You virus
Home page hijackings
New Ice Age virus
Hoaxes NOT related to computer security
The China Syndrome, part 3
Never had a lot to lose: Viruses for Fu Manchu
Every day is April Fool's
Done
Internet

9 Never open file attachments unless you are absolutely certain of their provenance. Try to avoid sending attachments unless absolutely necessary. Your friends may think you dull if you resist the impulse to send them the latest dancing bottles or cartoon sex, but imagine what they'll think if it happens to contain the latest example of a new virus that trashes their data. Also, resist the impulse to send the latest hoax virus to everyone you know. It's not news!



SecurityFocus - Microsoft Internet Explorer

Address: http://www.securityfocus.com

April 11, 2001

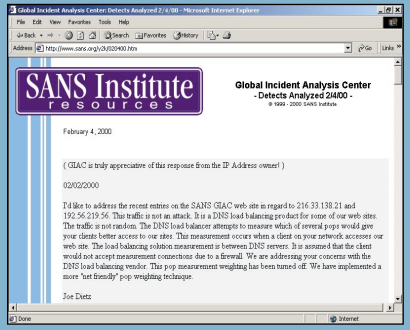
Internet Security and Your Business - Knowing the Risks

by Joe Jenkins (joe@nowalls.com)

last updated Nov. 6, 2000

In February 2000, denial of service attacks against web giants like Yahoo and eBay garnered a lot of attention from the media and from the Internet community. When it comes to problems with Internet security, it is usually major attacks against big companies that get the headlines. Unfortunately, many small or home business owners do not realize that they are just as likely to be targeted as any large company. As a consequence of existing in the digital age, almost everyone is vulnerable to breaches of security. If your business relies on computer or Internet technology, you need to be prepared to deal with security issues.

10 Read about it! There are literally dozens of security sites loaded with information on security threats, the latest virus alerts, and the security holes discovered in popular operating systems and applications. This information is available to all; you can bet someone out there is trying to put it into practice. For the best available real-world overview of security get hold of the book *Secrets and Lies* by Bruce Schneier or subscribe to his newsletter at www.counterpane.com.



Global Incident Analysis Center: Detects Analyzed 2/4/00 - Microsoft Internet Explorer

Address: http://www.sans.org/y2k/020400.htm

Global Incident Analysis Center - Detects Analyzed 2/4/00 -

© 1999 - 2000 SANS Institute

February 4, 2000

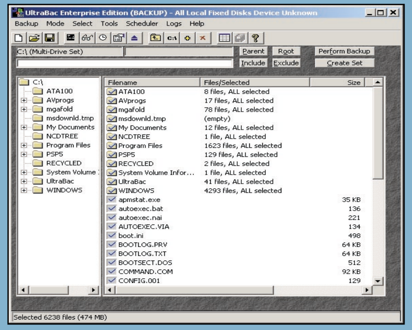
(GIAC is truly appreciative of this response from the IP Address owner!)

02/02/2000

I'd like to address the recent entries on the SANS GIAC web site in regard to 216.33.138.21 and 192.56.219.56. This traffic is not an attack. It is a DNS load balancing product for some of our web sites. The traffic is not random. The DNS load balancer attempts to measure which of several pops would give your clients better access to our sites. This measurement occurs when a client on your network accesses our web site. The load balancing solution measurement is between DNS servers. It is assumed that the client would not accept measurement connections due to a firewall. We are addressing your concerns with the DNS load balancing vendor. This pop measurement weighting has been turned off. We have implemented a more "net friendly" pop weighting technique.

Joe Dietz

11 Don't overdose on risk and assume that every unknown incoming transmission trapped by your firewall represents a threat. Lots and lots of 'threats' have mundane technical explanations. For example, many ISPs use special techniques to spread the load over several servers and this 'load balancing' technology can sometimes be mistaken for a real attack. The important point is that whether it's an attack or not, the firewall blocked it. That's why it's there – to stop you worrying.



UltraBac Enterprise Edition (BACKUP) - All Local Fixed Disks Device Unknown

C:\ (Multi-Drive Set)

```
Filename               Files/Selected              Size
ATA100                 8 files, ALL selected
AVprogs                17 files, ALL selected
mgafold                78 files, ALL selected
msdownld.tmp           (empty)
My Documents           12 files, ALL selected
NCDTREE                1 file, ALL selected
Program Files          1623 files, ALL selected
PSP5                   129 files, ALL selected
RECYCLED               2 files, ALL selected
System Volume Infor... 1 file, ALL selected
UltraBac               41 files, ALL selected
WINDOWS                4293 files, ALL selected
apmstat.exe                                       35 KB
autoexec.bat                                        136
autoexec.nai                                        221
AUTOEXEC.VIA                                        134
boot.ini                                            498
BOOTLOG.PRV                                       64 KB
BOOTLOG.TXT                                       64 KB
BOOTSECT.DOS                                        512
COMMAND.COM                                       92 KB
CONFIG.001                                          129
```

Selected 6238 files (474 MB)

12 Finally, backup, backup, backup! When things go bad it's the only way to recover quickly with a minimum of effort. The Backup program included in Windows is extremely basic. To make backup easy and automatic so that you don't forget to do it, invest in a fully featured backup utility, for example, the grown-up version of Windows backup from Veritas (www.veritas.com) or UltraBac from www.ultrabac.com. Always remember to do test restores. Nothing hurts like a backup that won't restore.

QUICK TIP

Move data files away from their default locations. This makes it harder for anyone who does manage to gain access to your system to discover them, and it will make data-only backups easier.

we all need to take precautions against such attacks, even if they don't explicitly target us or sites important to us, because the Internet reroutes around blockages and the impact of disruption anywhere ripples out across the network. When a JCB cuts through an Internet trunk route in Idaho, it's not unknown for the impact to be felt in the UK. There are many tools, both hardware and software, with which we can defend ourselves from these risks.

The most effective starting point for the home user is a combination of anti-virus protection (see June's anti-virus group test) and a personal firewall, but this should be accompanied by some self-education and an all-round update of Windows and Internet applications. A good anti-virus scanner will catch known exploits and if the scanner also detects suspicious behaviour (heuristic detection) it may catch some (but probably not all) new exploits. This is where a good personal firewall, designed to detect and block all outgoing transmissions except those that you have explicitly allowed, becomes your second line of defence. Unfortunately, most personal firewalls do not yet permit the fine-grained control you need to stop all potentially risky outgoing transmissions, and this is where you come in.

As the only person you can trust to make decisions about the level of security on your system, you can educate yourself by visiting security-oriented sites to learn about the vulnerabilities of your chosen software and the actions you can take to reduce your exposure. The page on Information Security Threats in the section titled 'The Basics' at www.securityfocus.com is a good place to start, and www.safer-hex.com has a good selection of news on various threats, plus news of risks and updates in operating systems and software.

We haven't said much about the ability of personal firewalls to block incoming threats because the principal benefit to most home users is the blocking of some of the more egregious security holes in Windows through which personal data or attacks on other computers may exit the system. Personal firewalls provide some benefit by discarding unsolicited incoming transmissions, but these do not always represent attacks on the system. In many cases they are benign, but personal firewalls don't usually provide enough information for the home user to evaluate the risk. A personal firewall is best treated as a quick fix and a primer on security issues. View incoming alerts as a prompt to research the cause rather than a significant risk and in most cases you will be right, provided you have taken reasonable steps to secure your system. PCW

QUICK TIP

If you use the Eudora email client, update to the latest version, then go to Tools/Options/Viewing Mail and make sure that 'Allow Executables in HTML Content' and 'Use Microsoft Viewer' are disabled.