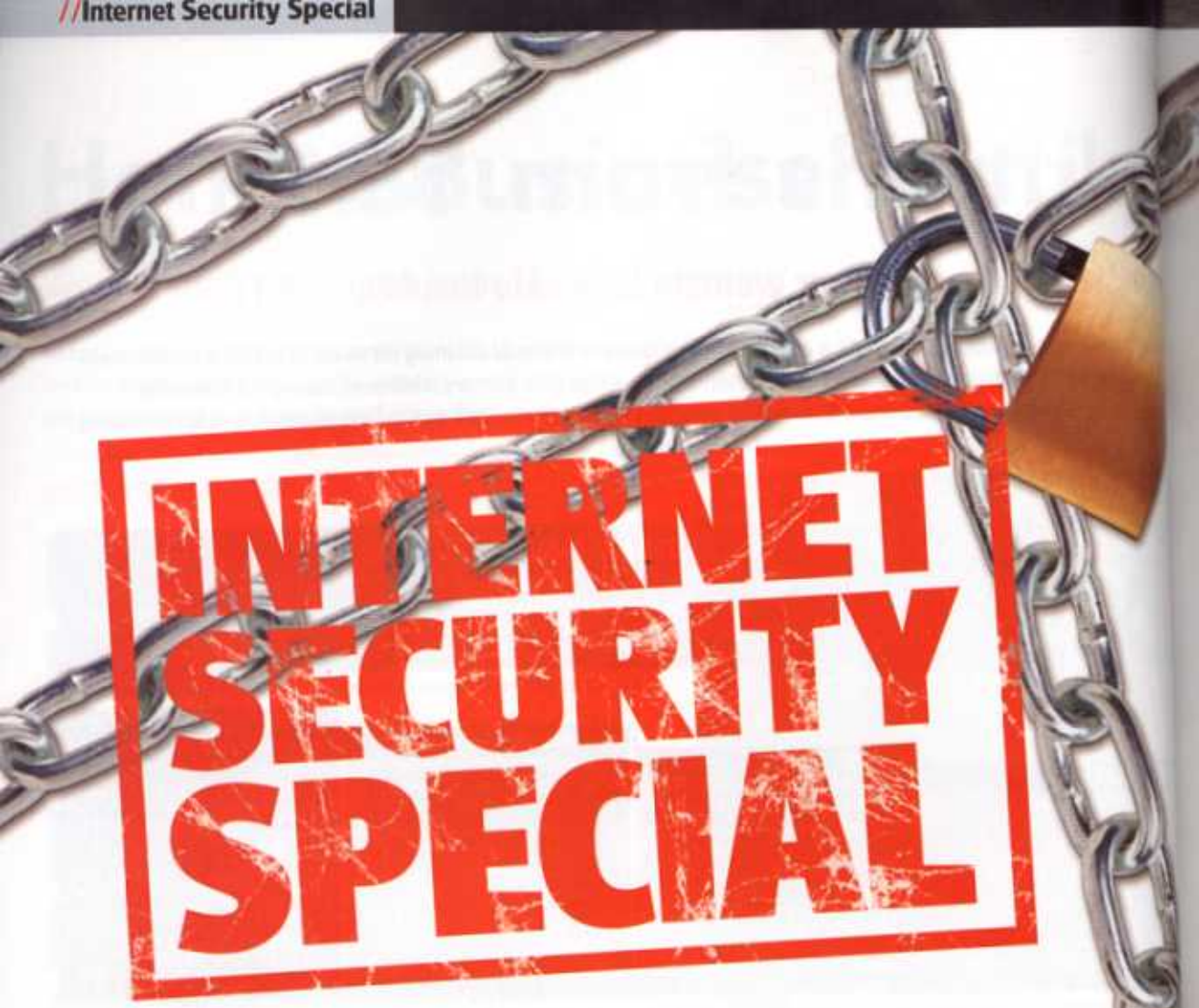

INTERNET SECURITY SPECIAL

SECURITY THREATS ARE RAMPANT ON TODAY'S INTERNET AND IT PAYS TO TAKE PRECAUTIONS. **DARREN LOCK** SHOWS YOU WHAT YOU NEED TO DO TO TURN YOUR PC INTO A VIRTUAL FORT KNOX

The Internet, so we're constantly told, is the gateway to the modern world. The most powerful reference source you'll ever use. The future of modern communication. Sadly, as with so many other things in the modern world, there are plenty of unpleasant things about the Net too. The very nature of the Internet relies on a two-way dialogue being established over a network, but there are many people who are out to use this line of communication to take advantage of your machine.

Take hackers, for instance. These unscrupulous programmers are constantly scanning the Net for open 'ports' that they can infiltrate to use for their own dubious means. If you install a firewall on your PC and monitor the number of times it gets 'pinged' you'll be amazed.

But hackers aren't the only threat to your security. The number of viruses that can infiltrate your system and cause havoc to your PC and files is multiplying all the time, and you'll need to be both streetwise and smart to keep the bugs at bay.

And what about spam? Junkmail has long plagued the inboxes of most Net aficionados, but recent studies suggest that the problem of unwanted email is getting worse. Much worse.

Don't forget spyware either. This relatively new phenomenon, which sneakily installs itself on your machine and sends information about you and your Net habits back to the firm that installed it, is potentially the most unpleasant of all Net nasties.

And with so much publicity in the newspapers recently, we hardly need to remind you of the importance of keeping your children safe while they surf the Net.

But don't worry – there is a way to fight back against these unseen enemies. Read on and we'll reveal all of the essential tips and tricks that you need to keep both you and your family safe on the Web.

Smash spyware

SPYWARE – THE PROBLEM

Spyware is a particularly insidious form of software snooping. It isn't malicious, in that it doesn't set out to take over your PC, but it's always working in the background, always monitoring your Net access. It can be used to access private information, but is mostly used to generate personalised ad banners.

With the introduction of Windows XP, Microsoft introduced a number of features that could be regarded as spyware. There's the error-reporting feature that creates a detailed report whenever your machine crashes and then sends it back to Microsoft HQ. Then there's Windows Media Player's ability to identify your PC to Web sites whenever you download and listen to music.

If you've downloaded certain shareware applications, in particular the peer2peer file-sharing application KaZaA, it is most likely that you've installed the Gator spyware on your computer (**www.gatoradvertisinginformationnetwork.com**). Gator consists of four modules; the main Gator application claims to autocomplete Web forms (this is totally unnecessary as Internet Explorer has been able to do this since version 5.0); OfferCompanion is the advertising spyware module that spies on browsing habits, initialises pop-up adverts and sends personal information back to Gator; Trickler is an install stub that downloads all the other components silently under the user's nose; and GAIN is the newest incarnation of the Gator spy module.

SECURITY ESSENTIAL

Name: Ad-aware
URL: www.lavasoftusa.com/aaw.html
Cost: FREE

What does it do?: This is a spyware/adware removal tool. Just run this once, follow the on-screen instructions and your PC will be free from the spyware menace. There's even a handy back-up feature so you can restore your settings if things go wrong.

Why is it so good?: Ad-aware gives you the ability to remove all spyware and adware software on your computer with a couple of mouse clicks. Easy to use and totally effective, it is surprising that this thing is still free.

There are few better programs for removing spyware scum than the excellent Ad-aware

It's sneaky, devious, and we don't like it much, but Gator keeps plugging away at your machine

Reading the signs

So how can you spot if your computer is infected with spyware? It's simple – if you suddenly start getting strange pop-up adverts appearing when you use your Web browser or your home page has been changed without your knowledge, you are being snooped upon. In fact, if you have used the Internet in the past seven days then it is very likely you have some spyware installed. It's everywhere.

Scare yourself by visiting CounterExploited and seeing just how full of security holes your PC is

SPYWARE – THE SOLUTION

If you're a Windows XP user and want to remain anonymous, there are a couple of things you can do to stop Bill Gates and his cronies snooping. The first is to turn off error reporting. To do this, right-click the 'My Computer' icon and select 'Properties'. Now click on the 'Advanced' tab, select the 'Error Reporting' tab and uncheck all the items on this page, including 'Disable Error Reports'. Next up, click the 'Tools' menu in Windows Media Player and then choose 'Options'. From here, select the 'Player' tab and uncheck the 'Allow Internet Sites to Uniquely Identify Your Player' box. These are just two ways of turning off XP's self-monitoring features. For more information, visit the XP-Antispy site (**www.xp-antispy.de**).

Be aware

One application you shouldn't be without if you are intent on removing all spyware from your PC is Lavasoft's AdAware – and you can download this wonderful little app from **www.lavasoftusa.com**. This free utility scans your Registry and all the software modules installed on your PC, and then identifies which ones have spyware capabilities. With a few mouse clicks, your machine will be cleansed of the pesky programs, but be warned, you should always back up your Registry before you start messing around with it. Luckily enough, AdAware lets you do this before the changes are made.

The rough and the smooth

Of course, AdAware will present you will a long list of applications, so how will you know which are malicious and which are harmless? For a rounded education in all this spyware, head over to the TomCat Internet Solutions site at **www.tom-cat.com**. This site has a full list of spyware applications and is also jam-packed with excellent information covering all areas of Internet security from viruses to firewalls.

SECURITY ESSENTIAL

Name: SpyBot
URL: http://security.kolla.de
Cost: FREE

What does it do?: This application not only removes spyware/adware, but it also removes keyloggers such as Desktop Detective 2000 and usage trackers that feature in popular software packages such as Paint Shop Pro and WinZip.

Why is it so good?: This is very similar to Ad-aware but it takes security that one step further, helping you to remove keylogging software planted by hackers and usage trackers installed in commercial products.

Worried by more than just spyware? Allow SpyBot to ease your troubled mind

Once you have removed all this spyware, you might suddenly notice that applications such as KaZaA will stop functioning. This is because spyware components are essential for the main application to run. To get around this, you could try KaZaA Lite (**www.kazaalite.com**), which has the functionality of the original, only without the spyware. Watch out, though, because KaZaA Lite is as black market as they come.

Experienced PC users should check out the CounterExploited site at **www.cexx.org**. Be warned – if you manage to digest all the frightening information on this site, you'll never want to use the Net again.

AntiSpy gives you the inside story on the spyware that pervades Windows XP

Beat viruses

Probably the most comprehensive and up-to-date anti-virus news comes courtesy of Symantec

VIRUS PROTECTION – THE PROBLEM

The very first computer viruses can be traced back to 1981, when the Apple II Operating System was placed under threat by the spread of pirated computer games. But it wasn't until 1990 that Symantec launched Norton AntiVirus, the very first anti-virus program.

During the 1990s, the popularity of the Internet increased, and so did the number of viruses existing in 'the wild'. In fact, by 1992 the number of known viruses increased to 1,300, a jump of 420 percent since 1990.

The most successful viruses have been email-based. Some of the more well-known include the Melissa virus, which replicates itself by raiding your email address book and sending itself to 50 email addresses stored there. Viruses often appeal to your vanity or your curiosity. The big virus of 2000 was The Love Bug, which introduced itself with the subject line "ILOVEYOU". In 2001, it was the Anna Kournikova virus that tempted you to look at pictures of the female tennis star. In both cases, the recipient received a nasty Visual Basic virus. Viruses can only work if you open or run an attachment, so the emails should be safe to delete.

Many of these email viruses are more irritating than harmful. They replicate themselves ad infinitum and clog up email servers around the world, bringing down networks. They don't damage your personal computer, but they do screw up the system for everyone.

Of course, the most dangerous viruses are the ones that damage your machine. Most mess up your Operating System, some reformat your hard drive and the worst scramble your PC's BIOS chip, fatally damaging the motherboard.

"Treat every email that enters your inbox with suspicion. If it contains an attachment and you don't recognise the person that has sent it, delete it."

The shadowy figures

So who is responsible for creating these viruses? In the very beginning, it was earnest young programmers trying to create self-replicating code, just to see if it could be done. Nowadays, it tends to be teenage code monkeys with colourful names like TeKCnOPunK or WarezWizard. To them it's the computer equivalent of tagging or graffiti in the real world. Then there are the amateurs or script kiddies, who just modify existing code to create their particular brand of mayhem.

If you do manage to contract a virus, there's a chance you might not even know you have one. Some are programmed to lurk in the background and activate on a certain date, while others run immediately. With self-replicating email viruses, there's a strong chance you'll receive an email from someone on your address book bringing attention to the fact that you've just sent them a virus.

VIRUS PROTECTION – THE SOLUTION

It can be quite difficult to spot if you have picked up a virus. You may experience your computer crashing or your Internet connection might slow down to a crawl with alarming regularity. Files and folders may be deleted or renamed and some applications may stop working altogether. These are just few of the signs that something untoward is happening inside your PC.

Not only does it riddle your machine with spyware, but KaZaA might infect you, too

If it is already too late and you've got a virus entrenched on your computer, there's one resource you should know about. Symantec's Security Response centre (**http://securityresponse.symantec.com**) has a list of the latest virus threats as well as a download centre that lets you download tools to remove certain viruses from your system. If you haven't managed to identify the virus, you can also run an online virus check from the Symantec site, too.

Observe and protect

So what can you do to protect yourself from computer viruses? Well the first thing is to make sure you don't put your computer at risk of infection in the first place. Every piece of email that comes into your inbox should be treated with suspicion. If it has an attachment and you don't recognise the person that has sent it, delete it. Your virus checker should also be used to scan any application or file you download from the Internet. Popular peer2peer file-sharing programs such as KaZaA are particularly susceptible to virus attack.

Always make sure that you have a decent anti-virus application installed on your system. You don't have to go out and spend lots of money, either – there are perfectly decent freeware virus checkers that will do the job. Check out AVG Antivirus from Grisoft (**www.grisoft.com**), which is an excellent freeware application that guards against virus intrusion and scans all incoming and

FIVE VIRUSES THAT SHOOK THE WORLD

APPLE VIRUSES 1, 2 & 3 (1981)
These were the pieces of code that introduced the world to the concept of viruses. They infected the early Apple II Operating System, spreading via infected pirate computer games.

JERUSALEM (1988)
This virus was unleashed on Friday the 13th, and has been duly activated every Friday the 13th since. It works by damaging **.exe** and **.com** files and deleting any programs that run on that day.

TEQUILA (1991)
This was the first widespread polymorphic virus to be found in the wild. It proved very hard to detect because polymorphic viruses change their appearance each time they infect a new machine.

MELISSA (1999)
This infected Outlook's Address Book, sending itself to 50 addresses, making Melissa the fastest spreading virus at that time. Its creator, David L. Smith, was subsequently arrested by the FBI.

THE LOVE BUG (2000)
Also targeting Outlook's Address Book, this deletes MP3 and JPG files on a hard drive before sending out username and passwords to the virus author Onel de Guzman of the Philippines.

The map on McAfee's site not only looks great, but gives some impressive data

outgoing email for extra protection. There's also AntiVir (**www.free-av.com**), which can detect and remove more than 50,000 viruses.

But remember to always have your anti-virus software running in the background at all times so it can keep a virtual eye out for incoming nasties. It's also a good idea to perform a system-wide virus check every week. This can be time-consuming if you have a large hard drive on your computer, so schedule it to happen when you aren't planning to use your PC.

Invest in safety

To get the best virus protection, try one of the commercial packages, which often boast features that are missing from their freeware cousins. Take McAfee VirusScan (**www.mcafee.com**) for example – the latest incarnation features a World Virus Map to keep you informed of global outbreaks and uses behaviour-based heuristic scanning to pre-empt new viruses. Meanwhile, Symantec's Norton AntiVirus 2003 (**www.symantec.com**) detects and blocks viruses in instant messaging attachments and utilises exclusive worm-blocking technology. Commercial products also feature auto-updating capabilities to ensure your software is watertight against new virus variants.

You want virus protection without spending a penny? Allow the people at AntiVir to oblige

SECURITY ESSENTIALS

Name: AVG Antivirus **URL:** www.grisoft.com **Cost:** FREE

What does it do?: This freeware anti-virus application will helpfully protect your computer from most virus attacks. If you leave it running, it will even check all of your outgoing and incoming email for you.

Why is it so good?: It gives you many of the features that you would expect to find on a commercial product and you get regular updates for free, too. You would be a crazy fool not to install this application.

Name: Kaspersky File Checker **URL:** www.kaspersky.com/remoteviruschk.html **Cost:** FREE

What does it do?: Are you worried that the file you've just downloaded is infected with a virus? If so, this Web site allows you to scan your files remotely without having any anti-virus software installed.

Why is it so good?: Again, if you haven't got round to installing any anti-virus software and you want a quick result with the minimum of effort, Kaspersky File Checker will deliver every time.

Name: Panda Antivirus Titanium **URL:** www.pandasoftware.com **Cost:** £25

What does it do?: Looking for a shareware anti-virus application that has all the features of a commercial release? Try the Panda range. Their apps are free to trial and only the daily virus definition updates are missing.

Why is it so good?: This is a very good alternative to Norton and AVG. If you fancy trying something a little different, and like the option of paying for the product, you should definitely give Panda a spin.

Name: Norton AntiVirus 2003 **URL:** www.symantec.co.uk **Cost:** £39.99

What does it do?: Norton AntiVirus was the first application on the scene back in 1990. 12 years later and the software suite is still going strong. If you want a no-nonsense commercial anti-virus product, try Norton.

Why is it so good?: If you don't believe that a free program like AVG Anti-Virus will protect your system, you must buy Norton's product. This is the leading product in its field and will keep your PC as tight as a drum.

Name: Trend Housecall **URL:** http://housecall.trendmicro.com **Cost:** FREE

What does it do?: If you are worried that your PC has already been infected by something unwelcome, pay a visit to this site. Trend Housecall will scan your computer and check for viruses absolutely free.

Why is it so good?: This site gives you the chance to run a PC healthcheck without installing a separate piece of software. Just a couple of clicks and you'll know if your PC is infected or not.

Name: Virus List **URL:** www.viruslist.com **Cost:** FREE

What does it do?: If you want to be kept up-to-date with all the happenings in the virus world, then check out this Web site. There's a daily news section and a virus calendar to keep you in the picture.

Why is it so good?: This is an extensive virus list that is constantly updated. If your paranoia needs feeding, this site will give it a regular four-course meal with its updates and wealth of news.

Name: VMyths **URL:** www.vmyths.com **Cost:** FREE

What does it do?: Not all viruses are dangerous or even real. Yes, there's a whole world of hoax viruses and this Web site documents them all and gives you some tips on how to spot a genuine virus warning from a fake one.

Why is it so good?: We've all received a virus warning that has turned out to be fake. This site proves that, although the majority of reports are true, there's no harm in being vigilant and checking your sources first.

Can the spam

SPAM – THE PROBLEM

Having your own email address is one of the truly liberating advances of our age. You can contact people on the other side of the world and never be out of touch with anyone. But every silver lining has a cloud, and in the case of email, it is spam. Basically, spam is electronic junk mail, and while the first few instances of it are quite intriguing, it becomes a personal bugbear in absolutely no time. And with the rate of spam mail almost doubling over the past year, it can be downright intrusive. This isn't just because it is junk mail – it's also because of the often adult nature of its content. As you can't control it, you never know what's going to turn up, which can be very embarrassing if you receive spam at work.

Dirty scum

Scumware is very similar to the spyware installed by applications such as KaZaA, but this time it takes the form of an add-on to Internet Explorer. Scumware works by hijacking links and legitimate advertising banners on the Web pages that you visit. If you click on one of these replaced banners or links, you will be redirected to a Web site that has paid up to be a member of this scumware list. Scumware modules currently operating include Gator (see the Spyware section), eZula's TopText, ePilot and Surf+.

Nobody likes spam at all. Get rid of it by using the tremendous MailWasher application

Then there are the Web sites that try to hijack your browser, firing off a multitude of pop-up adverts, stealing your email address, changing your home page to theirs and trying to persuade your PC to download an applet you don't want.

SPAM– THE SOLUTION

At the moment there is no cure for spam, but there are a couple of steps you can take to keep your email address safe. Many email addresses are farmed straight from the newsgroups, so if you are a regular contributor to a group, don't include your genuine email address. Leave it out, fake it or add something like 'removetosendemail' just to confuse the spam spybots. If you have a Web site, then there's a good chance your email address is on it and can therefore be farmed by spam generators. Visit the Anti-Spam Scriptmaker site (**http://assmaker.mybravenet.com**) to download an application that turns email tags into image files, which are undetectable to Web spiders.

It's great, it's simple, and it's on our CD. Turn to page 121 to see how to use Pop-Up Stopper

If you are looking for something to sort through your incoming mail, try the Mailwasher application (**www.mailwasher.net**). This detects spam, deletes it and then returns the offending message to the sender with an attached 'email address not found' dummy reply to confuse spam generators.

Nip it in the bud

To prevent the insidious practice of hi-jacking your home page settings, pay a visit to **http://pjwalczak.com**, the home of StartPage Guard. This software blocks any site that tries to change your home page settings and will restore them automatically if any changes are made.

The irritation caused by pop-up browser windows can be stopped dead by installing the free version of Pop-Up Stopper on our cover CD this month. It blocks both pop-up and pop-under advertising, letting you enjoy an advertising-free surfing experience.

You can also stop Internet Explorer from downloading malicious applets. In IE, click on 'Tools', then 'Internet Options' before selecting the 'Security' tab. With the 'Internet security zone' selected, click the 'Custom Level' button. Work you way through the list of options, changing the 'Reset To:' drop-down menu to 'High'. Now press 'OK' twice to return to your browser. Now you will be prompted whenever an applicatio wants to install itself on your PC.

SECURITY ESSENTIAL

Name: SpamPal
URL: www.spampal.org.uk
Cost: FREE

What does it do?: This is a tiny, unobtrusive email filter application, that will sift through your email and eradicate all that nasty spam. It relies on a database of known email spam sites and is compatible with any POP3 mailbox.

Why is it so good?: This is a great application because it uses a constantly updated database of known spam email sources and is easy to set up and run.

SpamPal shows that you can kill spam without breaking the system resources bank

FIVE WAYS TO SPOT SPAM

YOU'RE A WINNER!

Appealing to everyone's desire to get something for nothing, the email announces that you've been entered into a prize draw or have won an item of software in an online raffle. It's the 21st Century version of Reader's Digest junk mail, but far easier to dispose of – you don't need to tear it up, for a start.

ARE YOU SMALL?

The signature announces that you can get a bigger "insert body part here" by visiting the site and buying a particular product, usually accompanied by some questionable pictures to illustrate the point. There are variations on this theme claiming to cure baldness, impotence and every other human ailment.

TREATING YOU LIKE A BANKER

One of the oldest scams involves a letter from the president of a large African multinational company with a cash-flow problem. You are asked to bankroll them for which you will receive a huge payout. The con has moved onto the Net, so beware of Africans bearing gifts.

LOANS R US

It's good news. The subject line says that you've been approved for a loan, so can easily pay off all your debts. Of course, the loan amount is always in dollars and is never applicable to non-US residents, so you wonder why they ever sent this to you in the first place. Because it is spam, you fool!

XXX HOT GIRLS ALERT

Obviously, the majority of spam you receive will be of the pornographic variety. We're all friends here, but receiving an endless torrent of filth from a site you've never subscribed to is both supremely irritating and embarrassing if your wife/mother/sister walks in while you're trying to delete it.

Stop hackers

HACKERS – THE PROBLEM

Every single time you connect your computer to the Internet, you could be leaving yourself vulnerable to computer hackers. It sounds like the stuff of fiction, but these unscrupulous programmers spend a lot of time port scanning – using an application to search the Internet for computers with open ports to exploit.

There are many reasons why these hackers do this. The first is that they are looking for vulnerable computers to use as proxy servers, and ride on the back of your IP address. They effectively become invisible when they do this, and it means that they can do even more nefarious deeds without being noticed. Another reason is just to be nosy – they like to see what's on your computer and snoop around your email. The worst kind are just malicious: they deliberately go out of their way to damage your PC and block your Internet connection.

These kind of attacks are few and far between, as most of the port scanners out there tend to be the curious kind. However, some hackers are still looking to defraud you, gleaning personal details like credit card and ISP login information from your hard drive. So it is best to be suspicious of everyone and take no chances.

It doesn't get the same coverage as the big two, but Preventon does a fine job of protecting you

HACKERS – THE SOLUTION

In order to surf safely, you will need to install a firewall to prevent any unwanted attention from port scanners. The two most popular commercial firewall applications are Norton Personal Firewall 2003 (£40, **www.symantec.co.uk**) and McAfee Personal Firewall Plus (£20.95 per year, **http://uk.mcafee.com**). Other commercial applications include Preventon Firewall Pro (£24.99, **www.preventon.com**) and BlackICE PC Protection (£34.95, **www.iss.net/uk**).

Of course, there are freeware firewalls to save you some cash. The most renowned of these is ZoneAlarm (**www.zonealarm.com**), which provides excellent security. Two other alternatives are Sygate Personal Firewall (**www.sygate.com**) and Tiny Personal Firewall (**www.tinysoftware.com**).

Security as standard

Anyone running Windows XP can take advantage of the built-in firewall. To activate your WinXP firewall, click on 'Start', then 'Connect To' and right-click on your Internet connection. Select the 'Properties' button from the menu and click on the 'Advanced' tab. Make sure that the 'Internet Connection Firewall' box is checked and then press 'OK' to exit.

Once your firewall is up and running, it will monitor all incoming and outgoing network traffic on your PC. It does this by using various filters and rules to examine data, and if the filters flag any incoming packet data, it isn't allowed into your PC. Advanced firewalls will also monitor all the applications on your computer and will not allow an application to access the Internet without you giving prior permission.

"Every single time you connect your computer to the Internet, you could be leaving yourself vulnerable to computer hackers"

SECURITY ESSENTIAL

Name: ZoneAlarm
URL: www.zonealarm.com
Cost: FREE

What does it do?: This firewall application will keep out intruders, keep an eye on any applications trying to access the Internet and generally make sure you don't fall foul of hackers.

Why is it so good?: ZoneAlarm is the Web's premier free firewall. It is a robust, easy-to-use application that will give you the maximum protection for nothing.

You must know by now how much we love ZoneAlarm. It's great, free and easy to use

SECURITY ESSENTIAL

Name: WebVeil
URL: www.webveil.com
Cost: FREE

What does it do?: This site gives you the lowdown on how to surf anonymously using proxy servers, anonymous services and general privacy information.

Why is it so good?: The information contained on this site is aimed at the beginner and if you follow the excellent guide to surfing by proxy, you will be invisible on the Net in no time.

Want to browse the Web without leaving a trail of evidence? Check out WebVeil

ANONYMOUS SURFING

WHEN YOU CONNECT to the Internet, your ISP logs your every movement, but if you want to preserve your anonymity and surf the Web invisibly, there are a couple of options open to you. All Web anonymisers rely on the user using a proxy server to surf the Net. This is a third party server that stands between you and the Internet, allowing you to surf privately, as you hide behind the proxy server's IP address. You could search for a free proxy server (there are lists of them on the Internet) and set up your browser to use one of them. The main problems with using this kind of server are that they are often unreliable and will slow down your surfing experience.

To get around these limitations, there are pay services such as Anonymizer (£8) **www.anonymizer.com**) or Freedom Security and Privacy Suite 3.2 (£52 **www.freedom.net**). These allow you to download security software that you can also use privately or remotely, like on a work machine.

Alternatively, you could check out one of the free anonymous browsing services. You can try a selection of these at The Cloak (**www.the-cloak.com**), Silenter (**www.silenter.com**) and ProxyOne (**www.proxyone.com**).

For more information about anonymous proxy surfing, visit WebVeil (**www.webveil.com**).

Keep children safe

CONTENT FILTERS – THE PROBLEM

It's every responsible parent's duty to take charge of his or her child's Internet use. With the rising tide of pornography and the danger of Internet chat rooms, it makes sense to add another level of protection to your PC.

We have already explained how to stop pornographic email appearing in your Inbox (see the Scumware section), but there's a whole different world of unsavoury happenings out there in the World Wide Web. It can be quite tough keeping this unwanted material out of your home. With a TV set, you can easily reach for the 'off' switch whenever something inappropriate appears but with the Internet you can never tell when something disturbing or offensive will pop up. Remember – the filth is only ever one mouse click away.

While the majority of pornography appears on Web sites, it's Internet chat rooms and instant messaging that parents should keep an eye on. From the outside, chat rooms appear quite harmless, but it's here that your

Net Nanny is probably the best content filter out there. Check out our workshop on page 80

"While the majority of pornography appears on Web sites, it's Internet chat rooms and instant messaging that parents should keep an eye on"

child could be communicating with an adult pretending to be a youngster. Yes, it is scaremongering, but you have to remember that no-one is what they appear on the Internet, unless you've met them in the flesh first.

But there's no need to get too paranoid. With some careful monitoring, there's no reason why your children can't have a perfectly safe Internet experience.

CONTENT FILTERS – THE SOLUTION

There are many software solutions that can stop your PC accessing undesirable information. Known as content filters, these block out inappropriate material. They do this by using two different mechanisms – keyword blocking and URL blocking. Keyword blocking uses a list of words that are deemed offensive and if a page contains any of these words, it is blocked. URL blocking uses a list of banned Web addresses, which is updated regularly by a third party, and the software requires a subscription to keep the list up-to-date.

If you are using Internet Explorer then you can already use your Web browser's filtering capabilities. In IE6, click on 'Tools', 'Internet Options' and then select the 'Content' tab. Click on the 'Enable' button, under 'Content Advisor' to be taken onto the configuration screen. Here you can designate which content is to be blocked by the browser. You can even set up a list of approved or disapproved sites using this feature. For more information, check out **www.microsoft.com/windows/ie/using/howto/contentadv/config.asp**.

There are quite a few Web-filtering applications available; the most well known of these are NetNanny (£24, **www.netnanny.com**) and CyberSitter (£24, **www.cybersitter.com**). These commercial products have increased filter categories and their own content recognition systems.

Free protection

If you are looking for a free solution to this problem, there are a couple of applications that stand up well against their full-price peers. IProtectYou (**www.softforyou.com**) provides Internet Filtering/Parental Control as well as blocking chat and instant message sessions that contain inappropriate words. We-Blocker (**www.we-blocker.com**) may not be as advanced as iProtectYou, but it still offers protection from Net nasties.

Of course, no computer application can replace common sense and the ever-watchful eye of a parent. You would be foolish to put your total trust in a computer application to do your job for you. A responsible parent should never let their child use the family computer unassisted and it makes sense to always have the PC in a communal area of the house where any Internet use can always be casually monitored.

SECURITY ESSENTIAL

Name: iProtectYou
URL: www.softforyou.com
Cost: FREE

What does it do?: IProtectYou is an Internet Filtering/Parental Control package that provides concerned parents with control over Internet usage. You can use it to block emails, chat sessions and instant messages that contain inappropriate words, stops annoying ads, and/or restrict Internet time to a predetermined schedule.

Why is it so good?: This piece of software is packed full of features and will help a worried parent take control of their PC in no time. What's more is that it is matches commercial rivals while being absolutely free.

We love free software, and iProtectYou is one of the finest exponents out there

JARGON BUSTER

SPYWARE
Also known as adware, this is any software that gathers information from a user's PC in a covert fashion and uses the user's Internet connection to report this data back to a central server.

SCUMWARE
This title refers to software that hijacks Internet Explorer and modifies links, banners and URLS so that they bounce the user back to sites that have subscribed to their scumware database.

PORT SCANNER
Refers to a piece of software used by hackers that rattles through a predetermined number of IP addresses, on the lookout for vulnerable computers with open ports that can be exploited.

VIRUS
A piece of malicious code written to load itself onto your computer. They are man-made and self-replicating, often taking advantage of email address books to travel to other unsuspecting users.

FIREWALL
A software or hardware system designed to stop unauthorised access to a private network. They act as a barrier, monitoring all incoming and outgoing traffic, blocking anything suspicious.

INTERNET SECURITY SPECIAL

See pages 64, 76, 80, 82 & 120 for more PC security advice