

**AOL SAFETY & SECURITY**

# act!vated



Sponsored special from



Don't fall prey to internet nasties!  
Find out how AOL's new Safety &  
Security Centre can help you and  
your family stay safer online





# act!vated contents

## Competition

Win a Sony VAIO laptop, a PS2, a year's AOL Broadband and loads of other goodies in our exclusive AOL Activated competition

II

Centre and show you how AOL can help you enjoy the wonderful world of the web with complete peace of mind

## Introducing Safety & Security Centre

We take you on a step-by-step tour of AOL's Safety & Security

IV

## Safety tips

We conclude our guide to internet safety with a handy selection of useful hints and tips on how to stay secure when you're online

VII



# Safer surfing for all

With AOL's Safety & Security Centre, you can leave everyone else to worry about the dangers of the internet while you and your family surf the web more safely

With the number of scare stories in the press every day it's a wonder that anyone ever uses the internet or email at all. If it's not **phishing** and fraud that we're being warned about, then it's **spyware** and **spam** or the safety of our children. Thankfully, the truth of the matter is that, armed with the right knowledge and tools, the net is a perfectly safe place for both you and your family. And while most internet service providers leave it up to their customers to fend for themselves against all the online nasties out there, AOL goes a step further by providing a comprehensive suite of safety and security tools to every member as part of its service.

AOL's new Safety & Security Centre brings together an enhanced set of tools and features that can provide you with all you need to protect yourself on every side, alerting you to many potential problems before you've even logged on to the web. From a quick system diagnostic to a permanent shield from hackers, AOL supplies it all as part of the

package – and places you firmly in control.

You can put a stop to pop-ups, can the spam and even help to make sure your children aren't

exposed to unsuitable material while they're online.

Avoiding the net because of a few threats would be like staying indoors because it's raining, particularly since the web has so much to offer – online shopping, auction sites, cheap phone calls, music downloads and video on demand to name but a few. That's why AOL thinks it's important that you should be able to enjoy all of these things and more, safe in the knowledge that you and your children can be guarded against the bad stuff that the media likes to frighten us with.

Over the next few pages we'll be investigating how AOL can help you and your family stay safer whether you're surfing the web, sending and receiving emails or using Instant Messenger to chat to friends and family. Taking a look at each aspect of AOL's Safety & Security Centre in turn, we'll demonstrate how AOL can provide an all-round safer and more secure online experience.



# Introducing AOL Safety & Security Centre

Not only does AOL provide millions of subscribers with a quality internet service – it also keeps them safer online with the all-new Safety & Security Centre

With more than 2.3 million subscribers across the UK, AOL already has a solid reputation for providing quality internet services – all of which include free technical support, exciting features such as photo-sharing and Video Instant Messenger and a broad spectrum of content including news, sport, music and movies.

AOL has also made a big commitment to the safety and security of its members while they're online. In fact, with its brand new Safety & Security Centre, the latest version of AOL provides instant access to all the tools, features and information you'll need to help protect your equipment, your data and your family against potential hazards that you might come up against when you're connected to the net.

Pay a visit to AOL's Safety & Security Centre (AOL Keyword: Safety & Security) and you'll notice that it identifies six main areas for concern and provides advice and tools to help combat them. Read on to see what these are and how you can stay safer while you enjoy the web with AOL.

## 1. Curing viruses (AOL Keyword: Virus)

We are always being told to make sure that our computers are adequately protected against **viruses**, but it's amazing just how many people still leave themselves wide open to attack.

Viruses come in many shapes and sizes and the damage they do can range from mildly annoying messages right up to system crashes and loss of valuable data.

Most virus infections enter our PCs via emails, which is why AOL automatically scans all email messages and their **attachments** for potential bugs, such as viruses, **Trojans** and **worms**.

For further peace of mind, however, users should consider additional protection from infections that could come from not only email but other sources too – instant messenger attachments, for example, shared files, program files or data on CDs and DVDs. For that reason, AOL provides its members with a free trial of McAfee VirusScan Online™, which offers advanced scanning, quarantine and repair features.

Since more than 250 new viruses are created every month, even the best anti-virus protection is only as good as its last update. That's why McAfee VirusScan Online™ updates itself automatically whenever you log onto the AOL service, so that you're always protected against infection.

## 2. Spyware beware (AOL Keyword: Spyware)

Have you ever visited a website only to find that your browser's homepage has mysteriously changed without your permission? Or have you recently become the victim of suspiciously increased levels of pop-up advertising? If so, you could well have a spy in your system.

Also known as adware, the majority of spyware is produced with the sole



**Safety & Security Centre**

**Safer Online in Six Simple Steps**

**Help Yourself to Safety**  
Check your current safety status on the right, then take the simple steps below to optimise your online security.

1. Get complete [anti-virus](#) protection for your whole computer including attachments and downloads
2. Download and run [AOL Spyware Protection](#) to boost your privacy and improve your connection
3. Frustrate the spammers and clean up your mailbox with AOL's powerful [anti-spam controls](#)
4. Ward off hackers: [change your password](#) regularly and set up your [free firewall](#)
5. Arm yourself against [internet invaders](#), including pop-ups, phishing scams and premium dialers
6. Set up AOL's famous [Parental Controls](#) to help you protect your kids online

**Safety Status**

**Safety on AOL**

Email Spam Controls	On
Email Virus Protection	On
Web-Pop-Up Controls	Off
Parental Controls	On

**Safety on My PC**

Computer Check-Up	Last Run 14/11
AOL Spyware Protection	Running
Firewall Software	Detected
Anti-Virus Protection	Detected

**General Online Safety**

Review AOL's [Privacy Policy](#)

AOL Keyword: Safety

▲ Safety & Security Centre is a one-stop resource for staying safer online

purpose of monitoring your online activity. Spyware can find its way onto your PC via many different sources without you even knowing – through a program you have installed on your system, a virus infection or sometimes just by visiting a website.

These sneaky secret agents can report back email addresses, preferred websites and other personal information to help companies target you with annoying pop-up adverts and marketing emails. And to add insult to injury, spyware can slow your system down considerably and even cause operational difficulties.

Naturally, it's vital to block such intrusions, so AOL offers its members a program that can be downloaded and installed to check for and remove any unwanted spies. Best of all, AOL Spyware Protection is free for all AOL members.

### 3. Can the spam (AOL Keyword: Spam)

While there is no doubt that the wonder of email has revolutionised business and home communication the world over, junk email – or spam – has become an increasing hindrance. Spam has now reached epidemic levels, with many reports suggesting that the volume of junk email currently in circulation could outweigh legitimate mail by a staggering ratio of 9 to 1.

At its least harmful, spam is simply a massive inconvenience, with users having to sift through and delete reams of unsolicited messages to get to a handful of genuine emails. But spam also frequently includes material that's unsuitable for children and, worse still, junk mail is often the vehicle used by viruses, scams and other online evils to reach your PC.

With this in mind, AOL has included enhanced anti-spam features into the latest version of the AOL software. Indeed, most spam is blocked before it gets anywhere near your Mailbox, thanks to spam filters on the AOL network.

In addition, AOL members get the benefit of Advanced Spam Filtering, which is built into their Mailbox and is able to learn and become more effective as time goes on. Suspected spam is delivered to a dedicated spam folder in your Mailbox. Simply click on the 'Report Spam' button whenever you receive a junk message – the more spam AOL members report, the more effective the filter becomes. Additionally, you can filter out emails that contain certain words or choose to receive only mails from people in your Address Book. You can even block spam – the instant messenger version of spam – using AOL's IM Catcher tool (AOL Keyword: IM Catcher).

### 4. Behind the firewall (AOL Keyword: Firewall)

Broadband has brought the convenience of a fast, always-on internet connection to millions of homes. But a permanent link to the web brings with it its own set of vulnerabilities.

And if you think that **hackers** limit their interests to cracking corporate mainframes or government networks, then you're unfortunately very



◀ With AOL you can stop worrying about spam

▼ McAfee Personal Firewall Plus is free for all AOL subscribers



wrong. A lot of modern hacking activity is aimed at domestic PCs in an attempt to get to your sensitive data (such as your bank details), take control or affect the functioning of your PC, or eavesdrop on your computer activity.

It's not just hackers that we have to watch out for, either. The growth of broadband has also seen a marked increase in the number of Trojans that can slip onto your system unnoticed, as well as other internet activity designed to compromise your privacy.

But there's one way to put a stop to all of this – simply install a **firewall** and your computer will be inaccessible to these sorts of attacks. A firewall is a program that acts as a barrier between your PC and the internet, monitoring all the traffic that travels between the two and stopping anything suspicious in its tracks.

These days, having a firewall in place is so important that AOL offers McAfee Personal Firewall Plus™ as a free download to all its broadband members. McAfee Personal Firewall Plus™ runs in the background and prevents any unauthorised access to your computer.

### 5. Other internet invaders (AOL Keyword: Invaders)

Unfortunately, there are a few other things you'll need to be aware of on top of all the hackers, viruses and worms out there – namely pop-ups and scams such as phishing and rogue diallers. Thankfully, however, most of these can easily be avoided using a combination of the right tools, a little vigilance and a bit of common sense.

Pop-ups are the little windows – usually adverts – that sometimes appear when you browse the web. These can be not only a pain, but can also compromise your security if you're unlucky. A pop-up blocking add-in, such as AOL's Pop-Up Control Settings, is the best solution, allowing you to banish all such intrusions with a single click. AOL's Pop-Up Controls also let you add certain web addresses to an 'allowed' list to cater for websites where pop-ups are used legitimately as part of the site. You also have the power to block animated media separately from pop-ups.

Phishing, meanwhile, is a type of scam that involves a hoax email that looks like it comes from a legitimate source, such as your bank. Con men use this method to direct you to a fake website and steal sensitive information, such as your bank details and passwords.

Other scams include rogue diallers, which are small programs that hijack your internet connection and divert you to connect via a premium-



rate phone line, meaning that you end up with huge phone charges every time you log onto the internet.

If you're using tools like AOL's spam filter, pop-up blocker and firewall, you've already gone a long way towards preventing scammers from getting anywhere near you. But knowledge is the best weapon to use against scams, including those of an online variety. From directly within AOL's Safety & Security Centre you can find out all you need to know about phishing, rogue diallers and the like. And once you know how to spot a scam, you've reduced the chances of becoming a victim.

## 6. Children first (AOL Keyword: Parental Controls)

The web is a great place for kids – they can play games, email their friends and family and even get help with their homework. But on top of the safety and security issues we've mentioned so far, there are some risks that families in particular should be aware of.

If you want to make sure your children are able to take advantage of everything the web has to offer in an environment that is safe, nothing



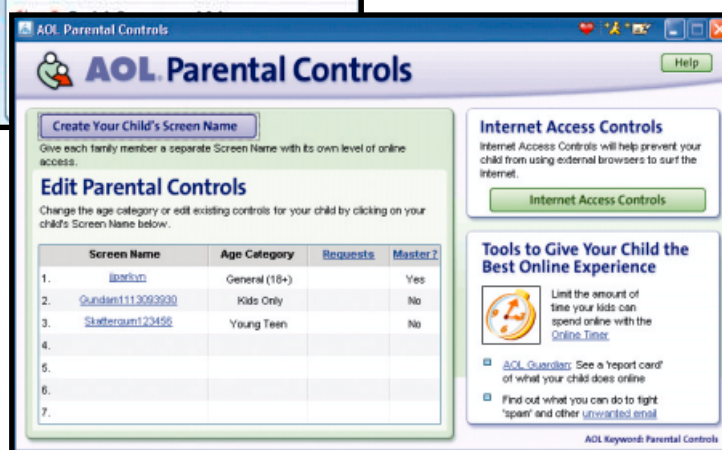
▲ Read up on all the dangers that you can be exposed to online

beats parental supervision and taking an active interest in what your children do online. As an added precaution, AOL provides all its members with built-in Parental Controls – they're easy to set up and they help to give you peace of mind.

Ideal for families, AOL's Parental Controls allow you to create separate logon identities (or Screen Name) for up to seven people and set privileges for everyone, based on how old they are and what you do or don't want them to have access to while they're online. There are four categories – Kids Only (12 and under), Young Teen (13-15), Mature Teen (16-17) and General (18+) – which restrict access to websites and services like instant messaging based on how appropriate they are for each age group. Parents can customise individual access to suit.

You can also limit the amount of time per day that each Screen Name is allowed to spend online and make use of a feature called AOL Guardian to report back to you on your child's online activities, including websites visited, emails sent and Instant Messenger activity.

AOL Guardian is by no means a covert method of spying on your kids, though, as children are always kept informed about what will be reported back to their parents. In fact, AOL Guardian works best when it's used as a starting point for open dialogue between parents and children about internet use.



▲ Set specific Parental Controls for each of your children

## Jargon Buster

Techno babble demystified

See [www.computeractive.co.uk](http://www.computeractive.co.uk) for a full list of Jargon Buster terms

**Attachment** A computer file, such as a word-processor document or spreadsheet, sent along with an email message.

**Firewall** A system that prevents unauthorised access to a computer over the internet.

**Hacker** People who break into other people's computers and networks, often in an attempt to steal sensitive information.

**Phishing** A form of internet fraud that tries to trick users into revealing personal details.

**Spam** Junk email sent to large groups of people offering such things as money-spinning ideas, holidays, and so on.

**Spyware** Software installed (usually surreptitiously) as part of another application installation specifically to monitor and report back on a computer's use.

**Trojan** A malicious program that's disguised as something else. For example, a Trojan may be disguised as a game when it's actually a program that steals your internet username and password.

**Virus** A program designed to cause at best annoyance and at worst damage to computer data. Viruses usually spread from computer to computer by 'infecting' files that are passed between them, or by automatically sending an email to everyone in your address book. They are often hidden in innocuous-looking files or email attachments.

**Worm** A program that transmits and copies itself over the internet. Not all worms are harmful but many are. Worms cannot attach themselves (or 'infect') other files.

# Top tips for safer surfing

Follow these simple steps to enjoy all the internet has to offer

**T**here are tons of ways you can help make sure your computer and all those who use it are safer from the potential pitfalls of the web. If you're an AOL member, a quick glance at the checklist on your Sign On screen will tell you whether you have adequate protection against spam, viruses, pop-ups and hackers.

If you're unsure about any of the settings, you can simply go to Computer Check-Up (AOL Keyword: Check-Up) and let AOL run a series of diagnostics to determine the safety of your internet connection and the general health of your PC. Most problems can be fixed automatically, while others can be tackled with the help of straightforward step-by-step guides.

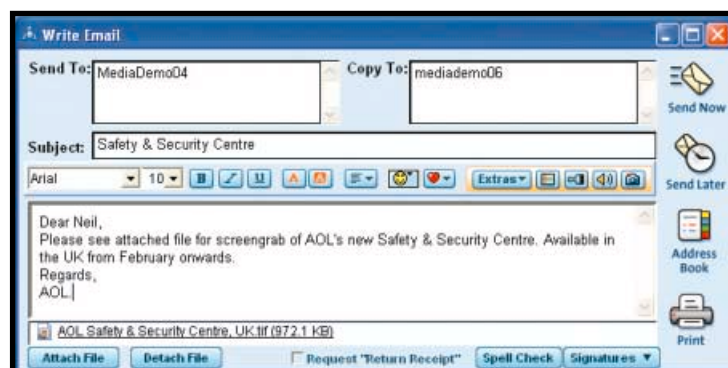
We have rounded up some hints on how to stay on top of your computer's security and be able to enjoy all that the web has to offer.

## Shop safely

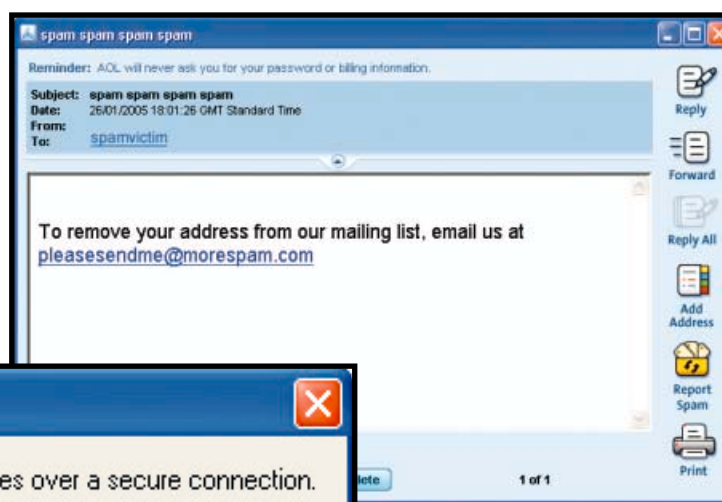
Online shopping is very safe – in fact, if you're careful it's safer than shopping on the high street. Stick to well-known outlets where possible, always use a credit card and before you enter any details check to make sure that the payment page you're using is secure. You can do this by looking for a small padlock icon in the bottom, right-hand corner of your browser window. Clicking on this brings up the site's security certificate, where you can double-check that the web address on the certificate matches the address on your screen. Also, a secure website's address begins with 'https' rather than just 'http'.

## Scan, man

Run a full virus scan at least once a week. Most anti-virus programs allow you to schedule full system scans, so make use of this and set your sweep to run at a time when you rarely need to use your PC. Similarly, if you have a spyware checker installed on your system, run regular spyware scans too. It is important to make sure your anti-spyware and anti-virus software is up to date, as new internet threats appear all the time.



▲ Steer clear of email attachments unless you're sure of their contents



▲ Don't reply to spam – it confirms that your email address is active

## Don't get attached

Never open email attachments if you're unsure about their contents, even if an email looks as if it comes from someone you trust. If you're using anti-virus software it will almost certainly stop any viruses

before they get to you – but it's best not to get too complacent, just in case.

## Ticking off

Be careful filling in online forms. Make sure you maximise your privacy by using the check boxes to opt out of allowing companies to use your details for marketing purposes or pass them on to anyone else. You can avoid a lot of spam this way.

## Spam scam

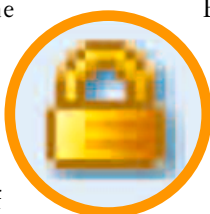
Many spam emails contain a link that says something like 'if you don't want to receive messages like this, click here' Don't do this! Replying to a spam message simply acknowledges that your email address is active and is likely to result in even more spam being aimed your way.

## Can't fool me

If you get an email promising you wondrous riches, it's almost certainly a scam. It might look as if it's been sent to you directly, but it's probably been sent out in an enormous batch of emails in the hope that one person out of thousands might fall for the con and relinquish valuable information, such as their bank details. Stay vigilant, maintain a healthy scepticism of any unsolicited mail and report any correspondence of this kind to your ISP.

## Phishing hook

Some emails sent out by scammers look really convincing, even using logos and addresses that look like they are official messages from somewhere like your bank, eBay or from payment services like PayPal. Don't let these tricks fool you. None of these institutions would ever ask for sensitive details in an email. Remember – if your bank genuinely wants to talk to you, someone will phone you up or write you a letter.



**For further information about AOL, or AOL's Safety & Security features,  
please go to: [www.aol.co.uk](http://www.aol.co.uk)**

