

Doctors Orders

Hello to all, Craig here again. Welcome to our April newsletter.

April fools day 2008 I was a raw trainee and I must admit, I spent most of the day running around looking for left handed screwdrivers and pink solder.

Now that I'm 12 months older and wiser I was determined not to fall into the same trap.

I needn't of worried, because since we launched our new super-cheap telephone technical support package all the engineers have been running around like headless chickens, which meant they had no time to torment me!

But by about 11 o'clock I was feeling a little disappointed, I started asking people if they needed a left handed screwdriver. Sort of like prodding the alligator with a stick when he it hasn't moved for a bit.

"Come on Craig, you can't catch me with that one, I know what day it is" was the reply.

They'd finally met their match! They've realised that I was a force to be reckoned with!

"Now's the time to get my own back" I thought.

It was 11.45am so I had to work quickly. One of the engineers had just got a new VW Golf and he had spent all week going on about how good it was, especially how quiet it was. I tied an old piece of cast iron drainpipe, that had been kicking around the yard for years, to the Golf's rear towing eye, and waited for him to go to lunch. Minutes later I saw the Golf go by the window, or should I saw heard it, because the racket it was making was deafening.

I was quietly chucking to myself when the engineer who owned the Golf came out of the accounts office. "What do you think" he said, "that 21 year old woman sales rep from yellow pages, has got a car just like mine and I've been saving for three years for mine, there's no justice".

I thought "Now would be a good time to go down the shop for my lunch", I sneaked out, but my bike that I'd left chained to the lamppost, was gone. "They can't have gotten that chain off the lamppost it was like anchor chain", I thought.

After walking around the yard for half hour, I realised that my bike was, technically, still attached to the lamppost... only it was at the top, 25 feet up.



Inside this issue

- [Online banking fraud up 132 per cent](#)
- [Antivirus2009 ups the anti](#)
- [Good Spyware?](#)
- [Firms ignoring internal threats](#)
- [10 worst April fool jokes](#)
- [Crooks exploit Natasha Richardson's death](#)
- [Channel 4 takes on the Internet Pornographers.](#)
- [Our Low Cost Online Support is a big Hit](#)
- [Easy way to resize many photos at once](#)
- [No reason to rush your upgrade to IE 8](#)
- [New Computer Doctors Toolbar](#)
- [Using valid characters in your e-mail address](#)
- [New image phishing method](#)
- [Anti-Spyware Roundup](#)

Online banking fraud up 132 per cent

New figures on fraud losses released by APACS, the UK payments association, have highlighted the need for proper online security as well as good internet security practices.

According to the data, phone, internet and mail order fraud otherwise referred to as card-not-present fraud has risen by 13 per cent in the last year by hitting £328.4 million from £290.5 million in 2007.

Protecting details from prying eyes online is also increasingly becoming vital as ID theft-related losses have seen a massive jump, recording a 39 per cent rise on 2007 to £47.4 million from £34.1 million.

The biggest leap has been recorded in online banking fraud losses, which have risen by a staggering 132 per cent, with losses totalling £52.5 million as a result of phishing and malware attacks.

Such online threats are the ones that are keeping pressure on the industry to continue reminding customers "to ensure that they have their computer's firewall switched on and anti-virus software installed and kept up to date", APACS said.

In addition CyberSource Corporation recently revealed that around £1.4 billion a year is lost to online fraud during the purchase of airline tickets.

Antivirus2009 ups the anti

A scareware programme is reportedly holding internet users to ransom and demanding money before allowing them to access their own documents, it has emerged.

Various internet security experts are warning that Antivirus2009 is now causing havoc to consumers by encrypting and holding victims' documents to ransom in exchange for a fee.

The rogue software scares internet users into downloading it by warning them through a fake Windows alert that their files are corrupt.

Afterwards those whose online security has been compromised by the malware are urged to download a programme named FileFixerPro, which is meant to sort out the problem.

However, once downloaded, the programme encrypts or scrambles folders in the machine, meaning that only those who pay for a FileFixerPro update can have their documents unencrypted.

Regular readers of our newsletter will know that we have been warning our customers of this piece of malware for some months. There are many incarnations of it on the Internet starting with "Antivirus2008" to "Antivirus 360" in each case it looks extremely plush and looks like a Microsoft or Norton site.

We've had several regular customers pick up this malware, some have even paid the money and some were even on our email list when we did our original emergency email, warning customers not to pay up.

Good Spyware?

If you think this sounds like a contradiction in terms then think again.

Spysure is a program used by parents and employers to track PC use.

It keeps a record of all web sites visited and key-strokes made (in effect a key logger!).

It can run in stealth mode so the unsuspecting child/employee doesn't even know they are being monitored.

Normally we wouldn't advocate any form of spyware but if your children run rings around your parental control software, (see page 4), you could try this.

The home version costs £39.97 but there is a free trial. Although, we are not sure if antispyware software such as Spybot will delete it as spyware.

<http://www.spysure.com/>

One customer told us that he never reads our emails as he finds computers boring. Fair enough, but he could have saved himself the £130.00 cost of reinstalling his computer just by heeding our warning.

Another question we are always asked is, "why me"?

In the old days, most malware arrived as an email attachment, but nowadays it nearly always comes from a website that is compromised or is paid by the malware writers to host it. Just clicking on the site gives you the malware.

So to be brutally honest, if you or your family visit websites showing pornography, illegal software including cracks for legal software or any of the peer-to-peer networking sites such as LimeWire, BearShare and BitTorrent, you're almost certain to pick up malware of some kind.

If you want to visit these sites, use a sandbox to protect your PC from harm. The best known of these is SandBoxie and can be downloaded from our download page.

www.computerdoctors.uk.net/pages/links.htm

Firms ignoring internal threats

New research has shown that small businesses remain focused on external internet security threats and are ignoring dangers from within posed by employees.

The research from online security firm GFI Software shows that only 22 per cent of respondents believe internal threats are more concerning, while some 50 per cent are not concerned about internal threats.

According to Walter Scott, the chief executive officer of the internet security firm says, "anti-virus and anti-spam applications can only help when it comes to tackling external threats".

"A secure network depends on many other factors and, unfortunately, the internal threat is far too often being ignored," he said.

"Endpoint security is absolutely critical even in the best of times, but with the economy prompting more and more redundancies, there are more disgruntled employees who pose a potential risk to an organisation's data."

The Ponemon Institute recently stated that six out of ten employees steal company data when they leave their jobs.

April 1st - here again

Did you spend the whole of Last Wednesday checking under your toilet seat for sheets of cling film or getting a willing volunteer to taste your tea just in case it was full of salt?



If you did, then you got off lightly.

If you think that you had a bad time this April fools day, then then take a look at this site to find the ten worst April fool jokes. Its amazing how, for one day each year, relatively normal human beings leave sanity at home for the day.

www.museumofhoaxes.com/worstaprilfools.html

Crooks exploit Natasha Richardson's death

Nothing is beyond the touch of cyber crooks when it comes to seeking victims to expose to online threats, even when the subject is as sensitive as death, it has emerged.



The heart-wrenching death of award-winning actress Natasha Richardson following a skiing accident in Canada is one such incident, according to online security firm Sophos.

In a blog posting on the subject, the firm's chief technology officer Graham Cluley revealed that compromised websites were being used by crooks to hit people looking for news on the death.

He said: "It appears that hackers are stuffing webpages with keywords - most likely scraping the content off legitimate news websites - in order to lure unwary surfers into visiting their dangerous sites and infecting their computers.

He went on to state that by filling their pages with the latest content on the incident, the crooks "make their attack quite timely and increase their chances of trapping victims".

Trapped victims risk having their computers infected by malware or even becoming victims of ID theft and online fraud.

All search engines use keywords to direct you to the correct site, so if you did a search for "Natasha Richardson" you would get a list of sites that had those words as their keywords.

Most sites would not use keywords that were not relevant to their site but the cyber crooks will use every means to get you to click on their "drive-by" site.

Once you realise it's not what you're looking for you click off, but too late, your PC is infected. The cyber crooks get paid by the spyware writers for every auto download. (See article on Antivirus2009, page 2).

The answer is not to just click on the first link you come to on a search engine. Look at the site name in the listing and see if it is either a well known site such as BBC or Microsoft or at least relevant to the search criteria that you have entered.

To help you in this you can download McAfee site advisor, it is available direct from www.siteadvisor.com. This will check every site in your search list against its database and give you a green tick or a red cross, depending on how the site is rated.

Channel 4 takes on the Internet Pornographers.



We make no excuses for covering this sensitive subject in our newsletter this month.

If you have children between the ages of 10 and 18 then this is your wake up call.

Now is the time to find out what your children are viewing in their bedrooms, while you're watching Coronation Street

We know people who are proud of the fact that they "don't know about computers and don't want to know". To these people we say: "You owe it to your children to make the effort to learn the basics of how to use a computer".

Most adults take light pornography as part of every day life. We are surrounded by it, in advertising on the television and newspapers.

But do not run away with the misconception that this is all there is on offer.

Channel 4 ran a series of programs last week to see where our children are getting their sex education from in the 21st century. You may be surprised to learn that its almost certainly not from their school, but from ... you've guessed it, the Internet.

But that sex education is nothing like the kind that you and I received when we were at school!

One of the presenters, in a live show, took a wireless enabled laptop and typed "porn" into a search engine to see what would happen. The first page viewed led to further links and within 2 minutes she had uncovered websites showing child sex and bestiality.

The presenter was so shocked that she refused to carry on and that part of the program was cancelled.

Instead they showed the results to a group of average parents in a private viewing, while the camera panned across the shocked faces of men and women who considered themselves broadminded.

You may say "This can't be true, images of this sort must be illegal" and so they are. Unfortunately, these images are housed on servers in the back alleys of the

world, run by organised crime gangs and even if their country's authorities have the inclination to shut them down, they would start up within hours at an alternative location.

These free images you see are not the main event, they are the tasters required to get you to part with your credit card details.

"Who in their right mind, would part with their card details to such a website", I hear you ask. Well if you leave your credit card accessible to your children, then YOU, is my reply!

As repairers we rarely get down to file level, we treat customers data en masse when backing up. We don't have the time or the inclination to view customer's photos.

But we can't help seeing the results of a visit to a hard porn site. This is in the form of heavy duty spyware that in some instances requires a full clean install to eradicate.

Don't get me wrong, the presence of heavy spyware does not necessarily mean the PC has been used to view pornography, after all there are plenty of illegal download sites for music and videos and sites for cracking software keys, that can give just as bad spyware.

The sole aim of the website owner is to make money by any means, the spyware writers pay for each visitor that gets infected.

You can't expect children to see the dangers, they might not "accept sweets from a stranger", but they'll see no harm in downloading the latest music track or having a laugh with their friends over some "rude pictures".

Its up to you to be responsible on their behalf, get involved with what they are doing on their PC. Let them see that making their own decisions on the sites they visit is not acceptable.

If you cannot control what your children view, then consider parental control software. There are some excellent free software packages available that will restrict the sites your children can visit. Its by no means perfect and its no substitute for a keen eyed parent, but it's better than nothing. It does require that you know how to use it unless you want an engineer round your house every month.

As most children are four or five times more computer savvy than their parents its not easy. It requires using a password that your children will not guess or obtain by other means. You will need to configure the software as your children find ways to beat it. (Don't forget they have a team of 12 year old computer geeks - their classmates - at their disposal).

And please, let no one utter those sacred words, "My children would never do anything like that" all I can say is "welcome to the real world".

<http://sexperienceuk.channel4.com/>

Our Low Cost Online Support is a big Hit

We were all a bit overwhelmed by the response to our new unlimited online support packages, namely "HomeCare" and "BusinessCare".

Even the, usually cynical, small business users have taken to it, realising the savings in cost and time that can be made having an engineer take over their PC and applying a fix over the Internet rather than getting an on-site engineer to attend.

Problems with home PC's can be just as exasperating but are usually a bit easier to fix, hence the lower cost of HomeCare (£6.99 per month) compared to BusinessCare (£9.99 per month).

Also many users have taken the optional advanced security pack (extra £2.00 per month) as this represents a bit of a bargain as the usual cost direct from the manufacturers is £48.80 per year. We only managed to secure it at this price by promising them hundreds of customers. Fortunately, a gamble on our part that paid off.

HomeCare users also get 20% discount on workshop fixed prices and on-site fixed prices if in our area.

Therefore the workshop fixed price for a standard PC repair falls from £68.49 to £54.79, a saving of £13.70, the equivalent of over two months telephone or online support.

Add to this the savings made by fixing your PC online against the cost of an engineer coming to your home or office, you can see the savings to be had over, say, a 12 month period.

If we take control of your PC over the Internet (with your permission) and fix your problem, there is no additional charge made other than your monthly fee.

Obviously, sometimes there is no alternative but to get an engineer to your door. If your problem is hardware related our tech support engineer would not ask you to open your computer case, unlike some companies tech support. (Dell please note)

Our online support gets dedicated telephone lines that will free up our normal sales and booking lines for more customers wishing to book an engineer or enquire about the progress of their workshop repair.

If you are interested in our telephone/online support please go to:

<http://www.computerdoctors.uk.net/care>

You can click through and purchase your first month's support on our website and we will contact you to arrange a standing order for future months. Or give our sales a ring on 01604 415984 and they will arrange it for you.

Easy way to resize many photos at once

One small downside to the ease of taking digital photos is that you can end up with lots of them.

Trying to resize or otherwise process them one by one is a real time-burner, as one of our customers discovered:

"I have a lot of photos in a file, all in JPEG format. I want to set up a PowerPoint show using them. However, each photo is much too big to fit into the PowerPoint frame. I can reduce the size OK, but only one at a time — and it takes time! Is there a way to reduce the size of all the photos at once prior putting them into PowerPoint?"

There certainly is. What you're looking for is a tool to resize a whole batch of photos at once. In fact, if you enter the phrase **batch resize photos** in your favourite search engine, you'll discover a wealth of options. Add the word **free** to your search if you want to filter out commercial tools.

For highest-quality batch editing, look at a top-tier program such as GIMP.

<http://www.gimp.org/>

This free, open-source application is complex though. Google's Picasa — also free — is very easy to use and can do batch edits, but I personally find it too limited; the program is primarily a photo organizer that does some light editing as a sideline.

<http://picasa.google.com/>

When I need a fast way to resize many photos at once, I use the venerable — and free — IrfanView.

<http://www.irfanview.com/>

The program lets you process whole folders of photos in a snap and gives you good control over the final quality, including the ability to sharpen or otherwise modify all the photos in the batch you're working on.

IrfanView doesn't offer the image-editing tools of Adobe's Photoshop or GIMP, but for basic photo editing and very easy, very fast processing of large batches of photos, the product is hard to beat!

No reason to rush your upgrade to IE 8



Microsoft touts Internet Explorer 8 as a big improvement over previous versions of the browser in terms of security, speed, and compatibility.

While that's basically true, the inevitable new-release glitches — which are already appearing — suggest you should wait at least a month before upgrading.

When you choose a browser, your first consideration should be security. There's no doubt that Internet Explorer is the target of more malware than any other piece of software. In fact, using IE is like painting a bull's-eye on your forehead and walking into a war zone.

Even though IE 8 adds some useful security features, its continued reliance on ActiveX makes the browser vulnerable in its very foundation. This lack of security is a primary reason many people have stopped using IE.

Security isn't the only factor causing Web denizens to flock to alternative browsers. For years, Internet Explorer's page rendering has caused major headaches for Web developers and users alike. Some pages that look and function as designers intended in Firefox, Opera, and other third-party browsers have their layouts broken when rendered by Internet Explorer.

IE 8 makes an effort to improve compatibility but ultimately falls short.

Performance is another area where IE has trailed the competition. Just as IE 7 runs faster than IE 6, the new version 8 is quicker than its predecessor. However, early tests indicate that IE 8 is still much slower than other browsers.

Compatibility improvements aid users and coders

IE 7 often jumbles the layout of sites that open and operate just fine in Firefox, Google Chrome, and other browsers. Web designers will be heartened to hear that IE 8 addresses many of these page-rendering deficiencies — and it's about time!

Constructing sites that work well in all browsers is definitely going to be much easier. Likewise, people who surf the Web will be less likely to encounter sites whose layouts are broken in IE 8. Without getting into the nitty-gritty, let me just say that IE 8 passes the Web Standards Project's Acid2 compliance test, as explained by the IEBlog.

<http://blogs.msdn.com/ie/archive/2007/12/19/internet-explorer-8-and-acid2-a-milestone.aspx>

Taking compatibility a step further, IE 8 includes a "compatibility view mode" that reverts to IE 7's rendering engine. You can toggle this mode on or off using a button near the search bar at the top of the browser. (The button icon looks like a broken document)

But there's a catch: IE 8 decides when to display the compatibility button. Obviously, if the button isn't showing, you can't click it. However, you can manually configure sites you want to view for compatibility by engaging the Compatibility View Settings option on the Tools menu.

If your organization uses custom intranet applications designed specifically for IE, you may need to adjust those applications to support version 8.

One of our customers reports that his intranet woes were not alleviated by using the new browser's compatibility mode. He had to force IE 8 into IE 7 mode by pressing F12 to open the Developer Tools and then selecting Internet Explorer 7 as the browser mode. These steps allowed him to sign in and use his company's intranet applications.

Microsoft provides a way for Web developers to handle browser incompatibilities on a page-by-page or site-wide basis. To force a page to render using IE 7 styles, end users can click View, Source and then change the header's meta http-equiv= setting to read as follows (be sure to retain the open and closed angle brackets at both ends of the tag):

```
meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" /
```

For site-wide rendering control, site owners can configure their servers to send the following HTTP header:

```
X-UA-Compatible: IE=EmulateIE7
```

Phishing filter upgraded to fight malware

Among the noteworthy security enhancements in IE 8 is the SmartScreen filter. This feature upgrades IE 7's Phishing Filter by adding a malware defence. (The Phishing Filter in IE 7 protects users against accidentally landing on spoofed sites and also detects other attacks that might try to steal your personal information.)

IE 8's new anti-malware component is a reputation-based filtering system. In this respect, it's like McAfee's SiteAd-

visor and Symantec's Norton Safe Web. Unlike SiteAdvisor, however, SmartScreen also works with signature-based technologies such as Microsoft's Malicious Software Removal Tool, Windows Defender, and others.

You can enable the browser's new InPrivate mode, which prevents IE from saving cookies, your browsing history, cache data, and other personal information.

IE 8 also offers better protections against cross-site scripting attacks and clickjacking, a hacker technique that tricks you into clicking on hidden page elements. Finally, Microsoft includes Data Execution Prevention (DEP/NX) memory protection in IE 8 to help prevent exploits that use memory tricks to launch malicious code.

However, none of these security features is foolproof. A prime example presented in early March at the CanSecWest conference is described in a Computerworld article. A researcher identified only as Nils compromised IE 8 running on Windows 7 by taking advantage of a shortcoming in the DEP/NX protection system.

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130683&intsrc=news_ts_head

More speed in IE 8, but not nearly enough

Microsoft would have us believe that speed isn't very important when it comes to page surfing. (Considering the miserable performance of previous versions of IE, that's understandable.)

Computerworld's JavaScript-performance tests show that Google Chrome is four times faster at JavaScript rendering than IE 8. In the same tests, Firefox 3.0.7 was 59% faster than IE 8 when rendering JavaScript on pages, Safari 47% faster, and Opera 38% faster.

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9130070>

So, does JavaScript rendering speed really matter? If you visit 50 such pages, and if they take an average of 2 seconds each to load, you'll spend an extra 60 seconds waiting in IE 8 than you would in Firefox. Over the course of a year, that's 6 hours of wasted time.

Of course, if you surf more than 50 pages a day, you could be wasting even more time with IE 8. In the business world, time is money, but time's even more precious in your private life. A browser's speed definitely matters — a lot!

There's no doubt that IE 8 is a much better browser than IE 7. Nevertheless, it's still inferior to Firefox and other alternatives. As to whether you should upgrade to IE 8 now or later, my advice is to use Firefox instead of either version.

If you must use Internet Explorer, I suggest you wait at least a month — two months would be better — before upgrading to IE 8. (If you're still using IE 6, however, install version 7 right away, for the sake of your security as well as for the added performance.)

Why do I think you should wait? At present, only a fraction of Windows users worldwide participated in the IE 8 beta. Now that the browser has been released to the public, it will be put through the wringer even more strenuously. When that happens, problems are bound to surface. For example, we've already received a few reports of odd page-load behaviour in IE 8 on Vista systems. And, bizarrely, some IE 8 installations revert to IE 7 after loading Windows updates.

Furthermore, the spyware writers are bound to start banging on the new browser even harder to unleash new exploits. Let some of that play out before you jump into IE 8 with both feet. Unless you have a compelling reason to upgrade to IE 8, just relax, wait, and watch what unfolds.

New Computer Doctors Toolbar

Are you concerned that the top of your browser window is full up with toolbars and only the bottom half is viewable. Of course, you can always right click on an unused area of the toolbar (Internet explorer) and untick the bars you don't need (for Firefox go to view/toolbars). Alternatively you could replace the whole lot with our new toolbar, its got everything you need. Well nearly.

All the local radio stations, news feed from BBC news, weather for the Northampton area, email notifier, quick links to our free download page and others, Google search bar and a gadget button where you can add extra links to a host of other plug-ins such as the YouTube top 10 and lots of different games to while away those lost minutes waiting for a download to finish.

You can even send us a free support email from the toolbar if you have a problem with your PC.

<http://computerdoctors.ourtoolbar.com/>

You need window XP, Vista or 2000 (no 98 or ME) and there are separate toolbars for Internet explorer or Firefox. Downloads and installs in seconds.

Using valid characters in your e-mail address

E-mail standards let you use characters other than letters and numbers in your addresses.

Unfortunately, various ISPs and webmail systems have differing rules governing which addresses are acceptable, making the whole area a bit of a mess.

E-mail address standards ignored by some ISPs

If you've ever sent an e-mail that's gone missing, or if you failed to receive a message someone sent you, it's possible that an invalid e-mail address was the culprit. The trick is in knowing a properly crafted address from an invalid one. This isn't as easy a matter as it may seem.

Allow me to demonstrate with this quick test: Which of the addresses below is invalid?

john.smith.@somewhere.com

All.Geeks.are." #\$\$%&*"[72.52.134.216]

From the point of view of Internet standards, the first rather innocuous-looking address is actually invalid, because it's illegal to have a full stop next to the @ sign. The ghastly-looking second address, by contrast, is perfectly valid, though it's unacceptable to at least one major webmail service — Hotmail — and probably others. To find out why, read on.

The allowable form of e-mail addresses is explained in an Internet Engineering Task Force document known as RFC 5322 and, to a lesser extent, in IETF document RFC 5321. These documents are pretty impenetrable, so let me translate the relevant bits into simple English for you.

An e-mail address consists of two parts separated by the @ sign. The bit to the left of the @ sign is called the local-part, and the bit to the right is called the domain. So if your e-mail address is joebloggs@hotmail.com, then "joebloggs" is the local-part and "hotmail.com" is the domain.

You may be surprised to learn that, according to the strict standard, the local-part is case-sensitive. That means joebloggs@hotmail.com is a different e-mail address from JoeBloggs@hotmail.com.

However, this part of the standard is ignored by most ISPs, webmasters, and webmail services, which usually treat the local-part as case-insensitive. This, as we shall see, is just one of several areas where practice rather than standards defines the validity of a particular e-mail address.

Another example is the use of special characters. According to the standard, the local-part can be up to 64 characters long and can consist of a mix of letters, numbers, or any of the following 20 special characters:

! # \$ % & ' * + - / = ? ^ _ ` . { | } ~

These characters, except the full stop, may appear anywhere in the local-part of the address. The full stop may not be used as the first or last character of the local-part nor twice in succession.

That may be what the standard says, but most e-mail providers avoid issuing addresses that contain these special characters. For example, many services allow only a single full stop to be used in the local-part of an address.

E-mail services often allow you to create addresses containing hyphens and underscores in the local-part, but this practice is far from universal. For example, Gmail won't allow hyphens or underscores. (Note that Gmail uses a plus sign [+] to designate throwaway addresses; more on these address extensions below.)

Likewise, the IETF standard allows up to 64 characters in the local-part, but very few e-mail services allow addresses anywhere near that long.

So we have a very strange situation: clearly, defined standards exist for e-mail address validity, yet the standards are largely ignored by webmail services, ISPs, and other e-mail providers, each of whom sets its own standards.

Real-world standards: Gmail, Yahoo, and Hotmail

I decided to find out exactly what e-mail addresses are allowed by the major webmail services: Hotmail, Gmail, and Yahoo Mail. There are actually two issues: which e-mail addresses these services will issue to users, and which addresses the services accept for outbound mail.

I was hopeful this would be neatly documented, but it's not. I had to conduct my own experiments, applying for new e-mail accounts to determine which addresses each service will accommodate.

1. **Gmail.** Google's Gmail will issue e-mail addresses only when the local-part is between six and 30 characters and consists of letters, numbers, and a single full stop. Furthermore, the first and last characters of the local-part cannot be a full stop. Oddly, a full stop within the local-part is effectively ignored, so john.smith@gmail.com is regarded by Gmail as the same address as johnsmith@gmail.com.

Once you have a Gmail address, you can expand it by adding a plus sign to the local-part and then some additional characters to create a throwaway address for signing up at questionable sites. Should that address become

a spam magnet, you can create a filter that redirects to your spam folder or trash folder any mail using it. Unfortunately, many of the web forms used at major sites don't recognize plus signs in e-mail addresses.

2. **Yahoo.** Yahoo Mail's system for creating temporary addresses based on your primary address is more practical. This is one of the reasons Yahoo Mail has the edge over competing webmail systems.

The local-part of a Yahoo Mail address must be between four and 32 characters and must start with a letter. It may contain letters, numbers, underscores, and one full stop but can't end with a full stop or underscore.

3. **Hotmail.** Microsoft's Hotmail service takes a different approach: the local-part must be between one and 38 characters long. It may contain letters, numbers, full stops, hyphens, and underscores. However, the local-part must start with a letter and must not end with a full stop. As with Gmail and Yahoo Mail, adjacent full stops are not allowed.

The conclusion is immediate. There are no universal standards; every mail system sets its own.

Only three characters are universally accepted

In the second part of my test, I tried to send an e-mail from Gmail, Yahoo Mail, and Hotmail accounts to a special e-mail address I set up at our Web site: `!#$%&'*+,-/=/?^_`{|}~@computerdoctors.uk.net`. That's a perfectly valid address from the point of view of the Internet standard, but it's well outside what's acceptable to these three services for their own users' addresses.

Both Gmail and Yahoo Mail allowed me to send mail to this strange address. Furthermore, the e-mail arrived at that account on our site's mail server. That's good news. It means that even though Gmail and Yahoo Mail are very restrictive in what addresses they're prepared to issue to their users, they're not as strict when it comes to e-mail sent from their system. In effect, you can send e-mail to virtually any valid address from these services.

With Hotmail, it was a different story. Hotmail would not allow me to send messages to my strange-but-legal e-mail address — I got an error message as soon as I pressed the Send button. I did a little experimentation, and it looks like Hotmail won't accept any special characters in an address you're sending to, with the exception of hyphens, underscores, and full stops.

If one of your friends has an address containing other special characters, you're out of luck.

I suspect Hotmail isn't the only e-mail service that won't let you send to legally valid addresses containing special characters.

How to craft a well-formed e-mail address

There are definite standards that define which e-mail addresses are valid. However, these standards are largely ignored by mail services, which instead define their own standards for the forms of address that are acceptable.

In this somewhat chaotic situation, your best bet is to use an e-mail address that everyone accepts — the lowest common denominator.

I suggest that your address start with a letter and that the local-part consist of six or more characters — letters and numbers only. Stay away from special characters, even though the e-mail standards permit them. That includes hyphens and underscores. The use of a full stop is OK, provided it doesn't occur at the start or end of the local-part. Avoid using two full stops, and certainly never have two full stops next to each other.

To play it really safe, stick with lower-case letters.

You may get away with using a more complex address, but by following the advice in this article, you're unlikely to have your e-mail bounce due to address-validity problems. As a bonus, you're never going to have your address rejected when registering at Web sites or signing up for newsletters.

New image phishing method

A new method to compromise the online security of internet users has been brought to light by internet security firm Arbor Networks.

The firm states that crooks have taken steganography, which involves hiding data in digital images, to the next level by embedding malicious HTML and java code calls in images.

Once done the images are then attached to phishing emails sent out to potential victims, says the firm, which claims to have discovered such messages doing the rounds.

Vulnerabilities in Internet Explorer's (IE) Multipurpose Internet Mail Extension (MIME) are apparently being exploited by the calls, which lead to the deployment of a fake login page purporting to be eBay's.

Due to IE's set up of scanning the first 256 bytes of a file being downloaded, the threat is able to get through because if HTML code is sniffed by the browser it will run it enabling the page to download.

According to Arbor, only IE seems to be affected by the issue because Firefox and Safari browsers display a broken image instead.

Important updates

If you use the Firefox and Opera browsers, make certain that you've updated your software to versions 3.0.7 and 9.64, respectively. These updates fix dangerous vulnerabilities in the programs.

Firefox 3.0.7 contains fixes for four security problems related to JavaScript, PNG image files, XML document data, and document object model elements.

Opera 9.64 contains three fixes that remedy security issues related to JPEG image files and JavaScript code, along with a fix for an "unspecified" problem for which no details were given.

An extremely dangerous vulnerability exists in **Adobe** Reader and Acrobat . A patch wasn't released until Mar. 11, so until you've applied the update, be very wary of opening any PDF files from unknown sources. If you have not had an auto update from Adobe visit www.adobe.com for the patch and install it without delay.

Anti-Spyware Roundup

We constantly get asked to recommend an anti-spyware program for older versions of Windows. This may reflect the growing number of spyware threats assaulting our older Windows systems and their lack of security updates.

Spybot Search & Destroy is a free tool supporting every version of Windows back to Windows 95.

<http://www.safer-networking.org/en/spybot/index.html>

Windows Defender is a free tool from Microsoft that requires Windows Genuine Advantage to download and use.

<http://www.microsoft.com/windows/products/winfamily/defender/default.mspx>

The only anti-spyware tool lacking a free version is Webroot Spy Sweeper, which costs £19.95 per year (discounts available for two or three years).

http://www.webroot.co.uk/En_GB/index.html

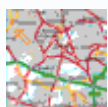
Finally, PC Tools Spyware Doctor has free and fee-based editions that work on versions of Windows from 98 up.

<http://www.pctools.com/spyware-doctor/>

Computer Doctors Ltd
Unit 12 Blackthorn Ind.
Est.
Blackthorn Road
Northampton
NN3 8PT

If this has been passed to you from a friend and you would like your own regular copy, just go to:

www.computerdoctors.uk.net/pages/newsletter.htm



Map to our Northampton Workshop
www.computerdoctors.uk.net/pages/map.htm

Contact us

General information & to book a call out

Tel: 01604 411 444 (9-6 Mon-Fri, 9-1 sat)

Sales & On-Line Purchases

Tel: 01604 415 984 (9-6 Mon-Fri, 9-1 sat)

Fax: 0871 251 9099

Email: sales@computerdoctors.uk.net

Shop: www.computerdoctors.uk.net/shop

Technical Support

Free: tech@computerdoctors.uk.net

Tel: 0905 121 1097 (9.30-4.30 Mon-Fri)
(Calls cost £1.00 per minute)

Web: www.computerdoctors.uk.net

Email test Facility:

mail.computerdoctors@keme.co.uk

