

# See the world as others see you



Is your website designed for access by colour blind people? Dyslexics? Or non-human visitors? Andy Wright says managers need to take e-communication very seriously indeed

**T**he web today encompasses virtually every part of the organisation. Managers across sales, purchasing, human resources, customer support, facilities, manufacturing and design all use the web to communicate with their 'customers' – both internal and external.

Today, every manager is a web manager.

All this means that the management community needs to understand issues like security, accessibility, usability and findability. It needs to look at how we communicate from the view of those we are communicating with – including the security-conscious, the disabled and even the non-human.

As users of the Internet we are all familiar with the increasing problems of data security. We encounter spam, phishing, viruses, spyware, malware and adware on a daily basis. And, with some justification, the IT industry and media at large have persuaded us that the Internet is a dangerous place. Evil-doers out there can invade our privacy, steal our identity, empty our bank accounts, convince us to join get-rich-quick schemes or sell us snake oil. They can borrow our computers to attack third parties like the Pentagon and Microsoft head office. Or they can simply mess up our computers, just for kicks.

Most Internet users have an armoury of tools to minimise the damage. If our service provider or IT

department does not protect us, we install security packages ourselves: spam filters on our email software (see fig 1), antivirus software, spyware blockers and firewalls on our PCs. We trust these tools to work. And we keep them up to date, don't we?

## THE VIEW FROM THE OTHER SIDE

Few, however, think about this paranoia from the other side of the fence. Yet anyone using the Internet to communicate needs to do just that, because every email that is sent will be treated with suspicion, all the way along the chain to its recipient.

Anti spam measures start with your service provider, specifically with the server that handles outgoing mail. For example, service providers like British Telecom (BT) will block senders it does not recognise. Its servers will only pass on mail from BT customers so if its 'From' address is not on their list of trusted accounts, the message will not get past first base. This is primarily to prevent spammers from hitching a ride and pretending to be someone else. It has the added benefit of freeing up resources and bandwidth for legitimate users.

The receiving email server has similar paranoid tendencies. Most mailboxes will filter out inbound mail from certain blacklisted domains, from mail accounts it knows are used by million-an-hour email merchants. This

should not affect legitimate emails, but sometimes it can, for a number of reasons. First, a spammer could use your outgoing mail server as a relay to hide their own identity. Secondly, your computer could have been attacked by a virus that propagates itself by highjacking your email software. Viruses like the notorious Worm.ExploreZip use Microsoft Outlook, Outlook Express and Exchange to mail itself out by replying to unread messages in the Inbox.

Finally, anti-spam software at the receiving end of the chain could stop your email getting through. Most anti-spam packages apply a range of different rules to filter out unwanted messages. Signs include: keywords such as 'FREE!!!', 'Dating', or 'Viagra' in the subject and message body, strange email addresses such as '123xyz@bt.com', foreign characters or blank lines in the email, and having a large number of addresses (or none) in the 'To' field.

## LEGITIMATE BULK EMAIL

The problem is compounded of course for those sending bulk emails. There are a few additional rules to ensure they not only reach their destination but also are read and accepted. Ensure that recipients have the option to remove themselves from the mailing list, and that the unsubscribe mechanism actually works. Offer a choice of HTML and plain text versions – many people will only read plain text messages because of worries that they will download

malicious material unknowingly. And remind people to add you to their list of known senders, or white list, to ensure they receive future emails from you.

Managers who use websites to communicate can fall foul of further security factors. If you are responsible for a website that uses cookies to track visitors, pop-ups, or code such as ActiveX controls or Java applets, consider carefully whether this will be acceptable to your target audience. Paranoid web browsers will block all of these. Also web masters need to ensure any security certificates, for example those used in for e-commerce sites, are up-to-date. All websites should have a privacy statement and other legal information, particularly if they fall under the scope of the Data Protection Act.

It all comes down to thinking about the website from the visitor's point of view. This does not just apply to the paranoid – web managers need equally to consider groups like those people with disabilities.

## ACCESS FOR ALL

Don't assume that all your visitors experience the web the same way. Some may not be able to see, hear or move and they may find it difficult or even impossible to process some types of information. Perhaps your audience includes those who have difficulty understanding text, and those that who aren't fluent in the language the document is written in. →



Technical issues can cause difficulties, too. For example, some visitors may not have a keyboard or mouse. They may have physical disorders or injuries making them unable to move a mouse or hit the keys.

And a lot of people use a text-only screen, a small display, or a slow connection to the Internet. Websites should also cater for earlier versions of the standard browsers, or for entirely different browsers such as voice synthesisers, Braille display, even for non-mainstream operating systems. Also, they may be in a situation where their eyes, ears, or hands are busy or interfered with (e.g. driving, working in a noisy environment, etc.).

Why is this important? Because the Disability Discrimination Act (DDA) of 1995 requires companies and organisations to make their websites accessible to all consumers. It is unlawful for “providers of services” to discriminate against a disabled person, and, since October 2004, organisations should have made “reasonable adjustments” to their websites to comply with the law, regardless of whether they are a blue chip company, small

### SPECIFIC REQUIREMENTS

Many partially-sighted Internet users rely on audio browsers. This means you should not depend on visual cues to navigate around the site. Designers use Alternative Text (ALT) tags as well as text-based links to complement the graphics. Text should be specified using style sheets, rather than fixed font sizes, so visitors can view large print if they need to. In addition, sites should provide an audio description of any video clips or animations.

Equally, visitors with impaired hearing or deafness require text transcripts for audio. This will also benefit surfers with slow Internet connections and those who struggle with spoken English.

To cater for the one-in-12 of the population suffering from colour blindness, the recommendation is not to rely on colour coding for conveying information: for example using red for ‘danger’. There are many resources on the Internet that address colour blindness issues, and the web has many resources can use a variety of tools to ensure their website is colour friendly.

Tabular layouts are the cause of major complications when using audio browsers. Guidelines recommend that tables should be correctly marked up to identify row and column headers and to ensure that data are presented correctly. Where tables are used simply to neaten the page layout, they should not confuse the audio browser into thinking that they contain data ordered in rows and columns.

There is no excuse any longer for excluding people. Checklists abound on the profusion of websites now devoted to accessibility issues, and there are software tools available – many of them free-of-charge – to check websites and repair them automatically.

There is a substantial up-side for all visitors. According to ‘The Web: Access and Inclusion for Disabled People’, DRC report published on April 14 2004, able-bodied people find that an accessible website is on average 35% quicker and easier to use than an inaccessible one. As a once-only exercise, making your website accessible may be time-consuming, even costly, but it will pay dividends well into the future.

### NON-HUMAN VISITORS

The third group of web visitors that need to be considered are the non-humans. A glance at your web servers visitor logs will show a great many hits from software robots – some good and some bad. The good ones are the so-called ‘spiders’ sent out by search engines like Google or MSN. You want to cultivate these because they are the ones that help people find their way to your site. Search engine optimisation needs an article all by itself to do justice to the subject, but the principles come down to one simple point: think about how they see it and give them what they want.

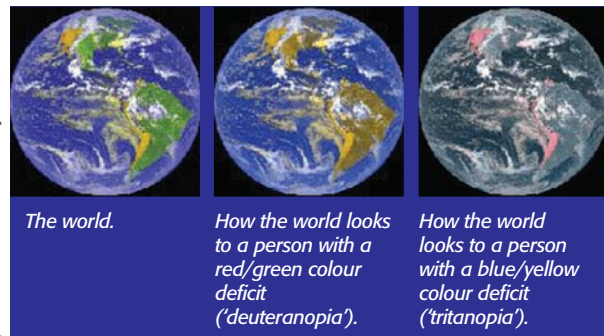


Fig 2: Colour blind people see web pages differently. See [www.vischeck.com/examples](http://www.vischeck.com/examples) for some more examples.

business, voluntary or public body. Recent surveys have shown just how ill prepared and unaware organisations are in complying with the legislation.

According to an in-depth comparison of the online annual reports of the S & P Global 100 Index, less than 10% meet basic requirements, and none of the top 10 national newspaper websites met a basic accessibility level, according to the national computing and disability charity, AbilityNet.

Ignoring these issues isn’t just discourteous or potentially unlawful. It could cost you business as well. You could be excluding the nine million deaf and hard of hearing people in the UK, six million dyslexics, two million blind and partially sighted and 1.8m people who experience colour blindness (see fig 2). Not to mention the 1.2m UK citizens with learning disabilities, seven million adults with only basic literacy skills, 450,000 people with epilepsy, 350,000 affected by strokes and 85,000 suffering from multiple sclerosis. You could be missing out on the estimated £40-50bn per year spending power of disabled people.

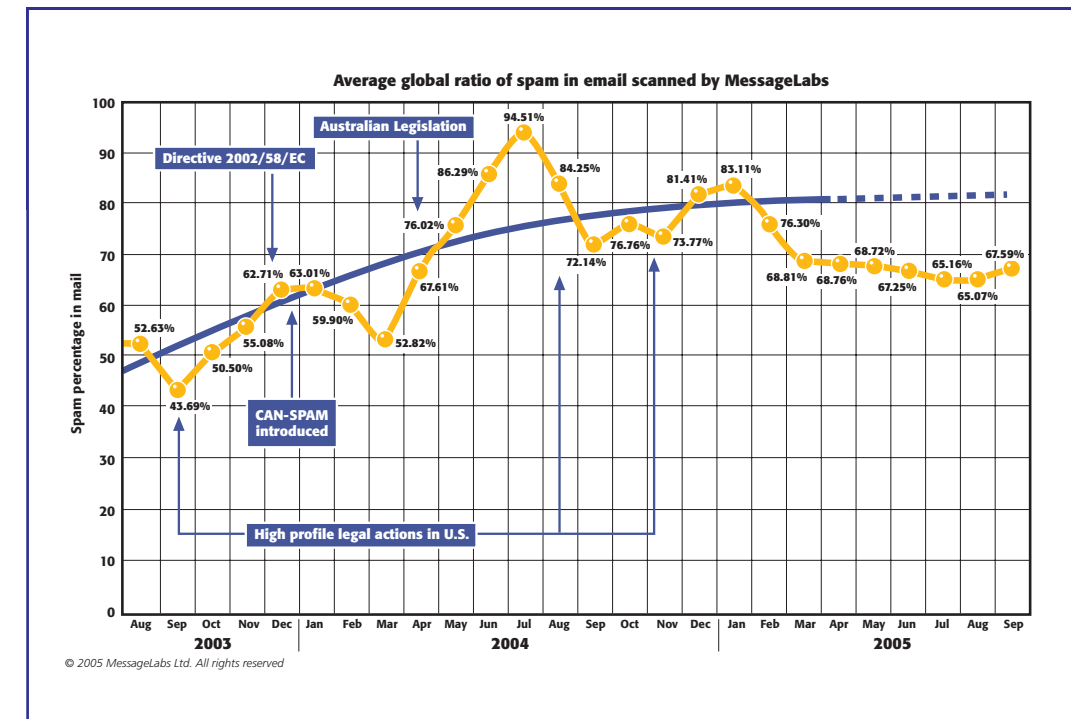


Fig 1: Spam accounts for nearly two-thirds of email messages.

[SOURCE: MESSAGELABS WWW.MESSAGELABS.COM]

Search engine indices like content. As with talking browsers, they like words – lots of them – and they assign meaning to the order in which they encounter these words. The earlier a word, the more important it is. Words in page titles are more important than those in the body text. Words in headings are important. But much-repeated words, text in tiny fonts, or rendered in the same colour as the background, are ignored because they are regarded as cheating.

As with humans, spiders like websites that are easy to navigate, aren’t too slow and don’t hide key information away. And, just as people like people who like people, search engines like websites that are popular: in particular they give higher rankings to sites that are linked from many other websites – especially from sites that themselves rank well. For example, a technical marketing company asked our agency to compare the Google ranking for several of its competitors. Most had a rank of 5 or 6/10 with 20-30 inbound links. One stood out with a higher ranking, but with just one website linked to it. The fact that it was linked from the Microsoft website was what made the difference.

Search engines change their rules frequently, aiming to provide better service to their customers, at the same time as staying ahead of those who seek to outwit them, to gain an unfair advantage and earn higher rankings than they deserve. So, like good friends, it pays to stay in touch, keep abreast of their likes and dislikes, and amend the site and its content accordingly.

Likewise, managers with web responsibilities need to pay attention to the less friendly, non-human visitors. One of the biggest nuisances are software agents that roam the web in order to harvest email addresses. These work at the behest of spammers and use some quite sophisticated technology to find new addresses for their masters. Techniques to combat them include masking the address in a script code, encrypting it, or displaying it as graphics. The most common method is to use a feedback form rather than email hyperlink to handle enquiries. This has the additional advantage of gathering information in a structured way. Fields can be validated, for example to check formatting of email addresses and postcodes.

Whatever your management discipline, the website can be your organisation’s most effective communication tool. Viewing it as others see it is the key. ■

**Andy Wright is managing director of Carino Communications, a web design, development and maintenance company focused on technology-based clients: [www.carino.co.uk](http://www.carino.co.uk)**

More information on disabled access from:  
[www.disability.gov.uk](http://www.disability.gov.uk)  
[www.drc-gb.org](http://www.drc-gb.org)  
[www.opsi.gov.uk/acts/acts1995/1995050.htm](http://www.opsi.gov.uk/acts/acts1995/1995050.htm)  
[www.mib.org.uk](http://www.mib.org.uk)  
[www.webcredible.co.uk](http://www.webcredible.co.uk)