

The need for filtering

Why the time is right for email and web content
filtering in the home and SME marketplace

by

Kevin Alexander
Managing Director
Trust Technology Services Ltd

Overview

The growth in internet usage and the increasing reliance on it for everyday tasks means that today the internet is one of the most important tools for both home and business. A business without email is like a family home without internet access - becoming more and more rare.

At the same time, the unscrupulous elements of the internet are enjoying unprecedented success. Pornography is number 1 in terms of traffic and income, and online gambling is increasing rapidly to catch up. The way in which these two industries in particular target new clients mean that the age of the viewer is almost impossible to determine. Pop-up adverts, spam email and fake links from seemingly safe websites are, in our view and others in the IT industry, the biggest threat to continued use of the internet.

To address this we need to find a reliable, consistent and configurable system that will allow granulated control over both web content and email.

This report will analyse the current problems and define the required solution. Wherever possible we will refrain from using technical jargon so that the report is understandable to a wide audience.

Internet access in the UK

As at 2004, 53% of UK adults have internet access at home. This is equivalent to 13 million homes, over 4 million of which are using broadband. In the small business sector over 68% have internet access and this figure increases towards 90% for larger companies.

The internet is no longer a luxury, but rather a way of life for the majority in the UK.

Major threats in the home

Children as young as 8 are currently expected to use the internet as a research tool for homework. If they stay within a defined set of internet sites then there is little risk of seeing inappropriate content, but a simple query on a search engine, or attempting to download some music will bring a much increased risk of seeing something offensive. Many parents are not as technically adept as their children and cannot watch over their every move on the internet.

A survey by a youth internet site, SmartGirl, of children with an average age of 13 ½ from the UK, Canada, India, New Zealand, Australia and the United States found that 49.5% are online for 1-3 hours per day. Over 60% had experienced adult material online. Many parents are simply unaware of the problem.

Email brings a whole new dimension. No longer does a home user have to search out offensive material, instead it comes direct into their mailbox. In our experience, it takes around 1 month for a new email address to be targeted by spammers. Email addresses are sold in bulk, or even guessed at by sophisticated software and once an address is on the list the spam increases almost exponentially.

Spam about cheap electronic goods is one thing, but the current spate of sexual growth tablets, gambling and porn site emails is concerning to an adult, let alone to a child viewing these kinds of things for the first time.

According to Brightmail, an internet email filtering company, there has been a 900% increase in individual spam attacks between April 2001 and April 2003. They also report that spam currently accounts for over half the worldwide email volume. A very small proportion of spam relates to indecent images of children. The Internet Watch Foundation (IWF) received 435 reports of indecent images sent via email in June of 2003.

Then there is the added risk of using instant messaging type software which is very popular with young teens. According to the Youth Internet Survey almost one quarter of children aged 10 to 13 years had received online sexual solicitations. Many of these are likely to be from adults pretending to be children.

This is a huge problem that will not go away whilst the internet companies behind it are continuing to make large amounts of money.

Major threats to business

Many people use the internet at work to book holidays, read news and chat socially with others. Whilst some companies will want to ban such activity it is difficult to enforce.

According to a survey carried out by the DTI, around one in five companies has experienced problems with employees misusing the internet. Nearly two-thirds of large companies reported an average of one incident a week.

A study by IRS Employment Review found that nearly a third of British businesses had taken formal action against up to five workers, while 21 percent had dealt with at least one disciplinary case in the last 12 months and five percent of businesses had punished over 6 employees for misuse of the internet.

Personnel Today magazine reports a quarter of UK companies have dismissed employees for internet misconduct. A total of 69% of dismissals were for workers surfing pornographic websites. Nearly three quarters of firms questioned had dealt with internet misuse, with chat rooms and personal e-mails coming second and third respectively in terms of most frequent complaints.

Interesting, over 50% of managers preferred to have a quiet word with workers and 29% used verbal warnings.

Recent court cases have highlighted just how difficult and time consuming it is to dismiss someone even for blatant distributing of pornographic images. Many companies are now taking the view that instead of monitoring and disciplining employees if they view the wrong kind of internet content, they want a system that simply blocks access to it altogether.

Email is another problem, and spam is particularly targeted towards companies since their email addresses are often displayed on websites. According to a report by the Oxford Internet Institute, 47% of internet users received too much spam, 23% had problems with obscene or abusive email, 18% experienced virus problems and 17% fraudulent activity.

Businesses need to be focused on business and be confident that their employees are doing the same. The current process of catching and disciplining is not efficient and can create serious long-term problems for companies. We believe the only answer is to block inappropriate content to ensure that misuse is no longer an issue.

The solution

Whilst the problems are slightly different for the home and business markets, the solution is the same. A system is required that can block certain categories of sites and filter email.

Software can be installed locally on home computers and each PC in a business, but this can be contravened fairly easily and needs to be updated frequently.

We believe a managed service run by an ISP that is updated centrally for thousands of clients, but yet is configurable for individual users and businesses is needed.

Growth of 5.3% is forecast in 2004 for Spam filtering software, with much of that growth expected in the managed filtering sector. According to International Data Corporation, the secure content management software market (which includes anti-spam products) will grow from \$236 million at the end of 2002 to \$1.1 billion by 2007.

However, on the ground in the UK the message is only just starting to be heard. A survey of London businesses found that just 34.2% use spam filtering software despite 78.9% reporting problems with spam email.

Small businesses are not keen to spend money on filtering software. Less than half (44%) of large UK businesses have spam filters in place, the overall figure including SMEs is 20%.

We believe this is about to change and that both homes and businesses will be keen to move to email and content filtering systems. In our discussions with SMEs and charities we see there is a huge requirement for a managed system. Without a filtering solution in place, families and companies are leaving themselves wide open to problems in the future.

A system such as that used by e-integrity (www.e-integrity.com) will become essential to both sectors over the next few years. We are committed to providing best advice to all our clients and as such will be recommending a filtering solution to each over the next few months.

Research

http://www.ofcom.org.uk/research/consumer_audience_research/telecoms/int_bband_updt/may2004/?a=87101

<http://news.zdnet.co.uk/internet/0,39020369,39118615,00.htm>
http://www.ofcom.org.uk/research/consumer_audience_research/telecoms/int_bband_updt/may2004/?a=87101

<http://64.233.183.104/search?q=cache:bfLTkhSzwF8J:www.broadbanduk.org/reports/Ofcom%2520InternetandBroadband%25200104.pdf+internet+oftel+percent+smes+uk+2004&hl=en>

<http://jobs.financialdirector.co.uk/News/1144452>

http://www.apig.org.uk/spam_report.pdf

http://www.wcit.org.uk/itprofession/prof_dutton.pdf

<http://www.smartgirl.org/reports/1934650.html>

http://www.unh.edu/ccrc/Youth_Internet_info_page.html

http://www.unh.edu/ccrc/pdf/Exposure_risk.pdf>

http://www.ofcom.org.uk/research/consumer_audience_research/telecoms/int_bband_updt/may2004/?a=87101

http://www.pchelpzone.net/news.php?oxynews_comment_id=15

<http://money.guardian.co.uk/work/story/0,1456,1195864,00.html?rss>

<http://www.startups.co.uk/YbRNPRhojdegVw.html>

http://www.gsec.co.uk/news/industry_news/2002/2002_06.htm

http://www.channelminds.com/article.php3?id_article=1476

<http://www.csoonline.com/metrics/viewmetric.cfm?id=588>

<http://66.102.9.104/search?q=cache:ldDOIzG2KV8J:www.londonchamber.co.uk/docimages/1027.pdf+%22use+spam+filtering%22+respondents+uk&hl=en>

<http://www.computerweekly.com/Article129700.htm>