

Fighting The Porn War

The rise of email pornography in the workplace

Ben White, CEO, MessageLabs

Earlier this year, an emailed jpg entitled 'Dirty Bushes' was intercepted in several US companies and found to be pornographic. Given the possible innuendo behind the name this probably doesn't sound too surprising, until you realize that the image was in fact a portrait of George and Laura Bush.

Perhaps you still aren't surprised — after all, who knows what goes on behind the walls of the White House? However, the image featured nothing more than the Presidential couple, in regal portrait pose, side-by-side and very much fully clothed. So how did it arise that a perfectly innocent emailed image of the President and his wife ever come to be thought of as indecent and unsuitable for viewing?

Corporate strategy

First, the reason that the image was initially flagged up as being inappropriate was because the companies in question were using a porn filter to analyse their corporate email traffic for pornographic content. On finding a dubious attachment, the said software either blocked the offending image or redirected it to someone of a higher rank who decided its fate. (As well as that of the unfortunate person that sent it!)

Now, it seems, more than ever before, employers want, and, more importantly, feel the *need*, to monitor their staff's email. In recent beta tests, my company, MessageLabs, found that 5% of all workplace emails have an attachment and that one in every four of those image attachments is pornographic — quite a startling figure and one which firmly establishes email as a prime vehicle for the distribution of porn.

The emailing of pornography within the workplace is not something to be taken lightly. Yes, it may seem like a bit of fun, but for employers across the world it does have serious consequences. There is the

issue of productivity — it is estimated that if each employee spends 12 minutes per day on non-work email, it will cost a firm of 500 employees £240 000 per annum (*Internet Use at Work*, 2000). This in itself would be enough to make most employers wince but for many a far more damaging issue is that of marred reputations and disgruntled ex-employees.

Over the last year there has been a string of high-profile dismissals involving large multinationals as a consequence of email porn. In October of last year 15 staff were dismissed from Merrill Lynch in the UK after they were caught distributing porn on the internal email system.

In January of this year, Royal Sun Alliance sacked 10 people and suspended another 77 over the distribution of a cartoon featuring Bart Simpson in pornographic pose.

And in June, a male employee from Dell was dismissed on grounds of sexual harassment for mistakenly sending an email containing nude photographs to a senior female executive in the US. He is now taking Dell to an industrial tribunal for wrongful dismissal.

But back to our image of George and Laura. On a less bureaucratic and more tangible level, the image of the Dirty Bushes was stopped because the porn filter in operation wasn't very sophisticated.

This is largely due to the software on offer — in the majority of cases the level of porn-filtering is, at present, very poor, with accuracy rates ranging anywhere from 20–70%. Current software relies primarily on skin tone, URL blockers and

text analysis. These methods have proven time and again to be ineffectual when it comes to intelligently filtering out porn from other harmless shots. The image of the President and First Lady was intercepted for no other reason that the wallpaper behind the Bushes was a creamy colour and therefore identified by the porn-filter as skin!

Such a situation is repeated daily, with no end of harmless pictures being rejected. This obviously creates a major problem for employers, especially given the fact that email has no regard for office walls or political or geographical boundaries.

In the past few years, email has become more than an additional communication aid, and many businesses would now struggle to survive without it. And the numbers are rising, with the number of Internet users set to grow from 45 million in 2001 to 215 million in 2003 (IDC, 2001).

When we think of the problems that such proliferation of email can cause, pornography is probably not the first thing that springs to mind. We are more likely to think of viruses (especially given the recent SirCam and CodeRed outbreaks) and may also feel that spam carries more than its fair share of problems. Looking at the problem as a whole, approximately 20–30% of all business email carries either a virus, spam or porn.

But, when it comes to reaction, porn is in a league of its own. Whereas viruses and spam are impersonal and inconvenient, email pornography is highly subjective and emotive, even menacing, and is certainly something which can cause some people real distress.

So, what can be done to minimize this relatively new problem? Perhaps the most crucial issue in this debate is surveillance — who should be responsible for the monitoring and blocking of porn within email?

Who is responsible

Should it be the ISP? This would seem a sensible option at first sight. The emotional burden of being the ogre of the office would be lifted (if only slightly)

from the employer — although whether employers would want the control of their email system taken away entirely from their control is unknown, but perhaps unlikely.

And whether or not an ISP would be willing to position itself as a 'smut-buster' for its entire customer base is also unclear.

Having ultimate responsibility for content is moving onto dodgy ground — a recent case in point being Demon's involvement in the Jamie Bulger case when the ISP found itself in danger of unknowingly breaching the injunction that bans the British media from reporting the new identities of the child's killers.

So, if we move away from the ISP level, what is left? The obvious alternative is to monitor and guard against such emails at the company level. Employers increasingly want to take responsibility — after all, they are the ones who are likely to feel the brunt, should their company suffer any kind of disgrace at the hands of porn-infested email or indeed at the hands of angry or distressed employees.

And surely, it is the employer who must make the decision if his/her employees are to be monitored and how closely. Company reputations are delicate and precious, as has been demonstrated by the previously cited examples.

But, if image-filtering must occur in the workplace, it doesn't follow that the office atmosphere should rival that of the Big Brother house. Employees may be less than enthusiastic about their email accounts being monitored, but porn-filtering technology is ultimately aimed at protecting them as much as depriving them of their entertainment and source of office gossip.

This is particularly the case with some of the cutting-edge image-filtering technology currently being developed. The benefits are two-fold. First, the new technology has the ability to differentiate between pornographic images and those which are completely harmless, such as holiday beach snaps and even artistic nudes. This is the area in which existing technology is seriously lacking. At present, image-filtering technology operates on an all or nothing basis, an image is either

showing skin or it isn't, it's either pornographic or safe.

Technological limitations

Of course, in establishing what kind of material should be let through a porn-filter and what shouldn't, the debate: 'What is porn?' inevitably arises. The boundary between porn and art has been argued since the creation of cave paintings, and there is no definitive answer — certainly I don't intend to impose one on you here.

Porn-filtering technology, however accurate, can never be all things to all people. What one person feels is deeply offensive, is shrugged off and dismissed — or even enjoyed — by another. Porn-filtering therefore is only as impartial as its creators and those developing new porn-filters can but make assumptions and generalizations on how society at large visually perceives art, pornography and glamour.

However, the second crucial feature that sets new technology apart is that it enables the employer to choose the level of censorship appropriate to his establishment. In so doing, different levels of prohibition are set according to the sensibilities and attitudes of any environment, and according to the audience receiving the email. For example, children accessing email in a school may require very specific regulations, while a model agency will need significantly less safeguards.

How does this new technology operate? The best technology we have come across is from First 4 Internet. It has developed an image-filtering service that in my view gives employers the best chance yet to get it right.

With an approved accuracy rate of 95%, the service uses textural analysis and a massive library of data to disseminate an image and identify exactly what is in it. The technology uses 22 000 different algorithms to define the content of any one image without hindering the speed at which the software operates, its artificial intelligence distinguishing between indoors and outdoors, posed

shots and natural, even landscapes and sea views.

Employers can take control of the email traffic passing through the workplace, choosing between 'high', 'medium' and 'low' settings so that the right level of censorship is obtained for any business. Equally, when an email is identified as containing a suspicious image, it can either be blocked or redirected to a server.

What this kind of technology offers above all is a flexible and realistic approach to image filtering in the workplace. It offers intelligent decision-making without bias. Employees can relax in the knowledge that they won't be apprehended for sending a friend or spouse a picture of their children playing on the beach.

Employers can also relax in the knowledge that they are making a concerted effort to protect their company from becoming embroiled in a legal case over email porn, as well as protecting the innocence of certain more sensitive members of their staff.

The day has come when email monitoring is a necessity, but this doesn't mean that the office should become a dictatorship. (I'm sure many would probably argue that their workplaces already fall into this category!) The focus for image-analysis is choice, flexibility and protection.

Most employers don't want to create unnecessary tension in the office, but they do want to establish an environment where they and their employees don't have to watch their backs. And where, if they want to receive pictures of George and Laura Bush, for whatever reason, they can.

About the author

Ben White is chief executive officer of MessagLabs, a leading managed service provider specialising in internet level email security. Part of the Star Technology Group, which Ben founded in 1995 along with his brother Jos White, MessageLabs has offices in the UK, USA and Hong Kong.