



Dealing with Facebook Phenomenon Effectively

by Graeme Pitts-Drake, Managing Director, Prefix IT

The tone of recent news stories about the dangers of Facebook has been quite hysterical and many IT directors can be forgiven for feeling under threat from the phenomenon. But is a blanket ban for the site the best approach or merely a knee-jerk reaction, perhaps a more tailored approach with network management tools is appropriate?

Dangers come in threes

In some regards, IT directors are right to be anxious. Facebook usage is horribly addictive and many users admit to spending at least two hours a day on the site during working hours. Not only is this a massive drain on productivity, it also hits company resources hard and opens up some significant security threats to boot.

Estimates from some organisations are quite alarming; a figure of £130m per day in lost productivity for UK businesses has been widely referenced and this is probably the key reason why 50% of employers have now banned the site completely.

192.com, the search engine, decided to prohibit the site completely after it was discovered that add-on applications used by 'Facebookers' were absorbing 40% of the company's available internet connection.

Hackers have of course cottoned onto the infiltration opportunities that Facebook presents and the coming months will doubtless see an increasing number of security scares. Personal security is also a potential minefield as many users are blithely sharing personal information on Facebook which could fuel identity theft and phishing attacks. News now comes that Facebook has agreed a deal to make users' names and photos available on Google, Yahoo and Microsoft search engines.

The newest face of online skiving?

However, in principle Facebook usage is just the latest in a string of online activities which can erode office productivity if not managed correctly. Companies have had to grapple with these from the earliest days of simple web-surfing through to YouTube, eBay, MSN and MySpace. Doubtless, before the year is out there will be new contenders; rumours of Google's entry into the market are just starting to circulate, so watch this space.

Facebook is so addictive because it is continually offering new activities and it's this multi-dimensional element that makes it so sticky. More than updating their own page and status, site users can now spend hours sending virtual gifts, playing Tetris (sic), opening fortune cookies, adopting an online pet, or throwing food at their friends, as well as tracking down old girl/boy-friends and 'poking' them which for many is the real point of this giant singles network.

PrefixNE

Power and control over your network assets
all wrapped up in one complete solution



Time to (over-) react?

Problems of over-use arise when staff abuse their access to these sites and are unclear about what is permissible and what is not and what the potential risks and penalties may be. Many companies are poor at devising appropriate policies for online use and worse at communicating them or getting employees to sign up to them.

The quick solution may be to ban Web2.0 sites, or block their access completely, which can be easily achieved with network management tools, but in so doing employers may face a back-lash from staff. Of course employers may be entitled to ban Facebook type sites outright, but this may well be an over-reaction. After all, few employers would begrudge workers a few minutes at lunchtime organising their social lives – as they would on the phone or in person. However, everyone's idea of 'reasonable use' is not necessarily the same and this is where clear policies and policing comes in.

Some lateral-thinking firms have provided access to Web2.0 applications on special PCs in communal staff areas which can only be used on breaks and during lunchtime.

Although a PC undoubtedly belongs to the company, users have also come to feel some sense of ownership and feel entitled to use their PC and its tools, for their own ends. Whether it's downloading pics and wallpaper to personalise a work PC, or using email to organise social activities, use of a PC is certainly seen as a perk, if not a right by most office workers.

Acceptable usage policies which are communicated and policed effectively are the key to managing all these behaviours correctly. Policing is important too, and monitoring employee internet usage is merely prudent. Some applications or sites should be prohibited, whilst others can be allowed in moderation, for instance at specific times, and both approaches can be achieved easily with network management tools.

On the plus side...

Those organisations that ban Web2.0 applications may not be acting in their own best interests in the long-term. In some companies there are reports of Facebook and other IM applications being used very effectively as business tools for collaboration, in preference to traditional email. It's easy to see that these technologies, which are on the verge of being outlawed, may well become accepted business tools in the near future.

Trying to close the door to Web 2.0 apps such as social networking, instant messaging and webcams is like being the doomed sorcerer's apprentice who eliminates one problem only to find two new ones taking its place. Better by far to educate staff on what is acceptable, what isn't, as well as the likely consequences. It would be naïve to leave it at that and trust staff implicitly, and there is a clear necessity to police internet usage, so that any infringement can then be dealt with quickly and appropriately.

Find out more about PrefixNE and how it could benefit your organisation at www.prefixit.com