

# **GFI** WHITE PAPER

## **SOCIAL NETWORKING AT WORK: THANKS, BUT NO THANKS?**

Millions of people around the world with access to the Internet are members of one or more social networks. They have a permanent online presence where they create profiles, share photos, share their thoughts with friends and spend hours just catching up with what hundreds of friends are doing with their life.



Give most people access to the Internet and they will spend the next hour checking their email, their Facebook profile, their MySpace webpage, updating their Twitter account and their LinkedIn account. It is addictive, occasionally fun and it does bring to light a lot of 'lost' contacts.

But the positives aside, if you own a business would you want your employees to be so keen on social networking that they could be spending unacceptably long periods of time online and chatting? No. And while most employers are willing to close an eye to the occasional quick browse and update, they are more concerned about those who abuse the system.

This brings us to the all-important question: What should I do?

Weighing the pros and cons of social networking at work can help businesses reach a decision that in the first instance safeguards the company's interests yet also takes into consideration the 'needs' and practices/hobbies that today's employees have.

### The Pros

1. Used diligently, social networking sites can be useful in expanding market reach, widening the business's circle of contacts, creating a communication platform with clients and advertise for free.
2. They can help a business to reach out to new markets, remain in touch with existing customers and use the snowball effect to market its services or products.
3. A positive presence online can boost a business's reputation and establish the name in new areas before taking the 'physical' plunge.
4. Social networking is a free source of marketing and advertising. The only cost to the business is the time and effort required to maintain the network and the official website.

### The Cons

1. The main concern for organizations is not social networking sites per se but the people using them. Social networkers are the weakest link and their actions can create problems. Computer users' actions are often based on impulse and not genuine awareness of what they are doing.
2. The P-word. Productivity. One reason why social networking sites are given a cold shoulder is the fact that employees could be spending unacceptably long on these sites. If every employee in a 50-employee company spent 30 minutes on social networking every day of a working week, that would total a cumulative productivity loss of 6,500 hours in one year. Now when you factor in how much each hour costs in salaries, you get a better and convincing picture. There is also an effect on company morale. While everyone sneaks a peek at his or her profile during the day, most employees would frown upon those whose social networking profile is open throughout the day. Morale is further hit if no action is taken.
3. Although updates to social networking sites may not take up huge amounts of bandwidth, the availability of (bandwidth-hungry) video links posted on these sites (or links taking users to sites like YouTube) creates problems for IT administrators. There is a cost to Internet browsing, especially where high levels of bandwidth are required.



4. The threat from web-borne viruses and malware is often overlooked by businesses. Hackers are attracted to social networking sites because they see the potential to commit fraud and launch spam and malware attacks.

There are tens of thousands of applications available for Facebook (according to the company) and while Facebook may make every effort to provide protection against malware, these third-party applications may not all be safe. Some have the potential to be used to infect computers with malicious code which in turn can be used to collect data from that user's site. Messaging on social networking sites is also a concern and the Koobface worm is but one example of how messages are used to spread malicious code and worms. A worm infection is the last thing an administrator wants to have to deal with! If you want to learn how to protect yourself from these threats, read Microsoft MVP Brad Dinerman's detailed article here:

<http://www.fieldbrook.net/TechTips/Security/SocialNetworking.asp>.

5. Social engineering is a fine art and a lot of people are falling for online scams that appear genuine. The scope is to take information from users using subtle methods. For example, a quiz asking 20 questions about you, your lifestyle and habits, could provide the answers required for identity verification purposes on other sites. Telling everyone what your favorite pet's name is may be harmless but you may also have used that as a secret question on a site to remind you what your password is. Simple and clever.

People also have a habit of posting details in their social networking profiles that beggars belief. While they would never disclose certain information when meeting someone for the first time, they see nothing wrong with posting it online for all to see on their profile, personal blog or other social networking site account.

People often post messages without thinking through what they have written. A seemingly innocuous message such as 'I'm working this weekend because we've found a problem in our front-end product' may be a spur of the moment comment but could raise concern among customers who may use that system, especially if the company handles confidential or financial detail.

6. Although there have been no major corporate lawsuits involving evidence from social networking sites, businesses need to be observant for employees who may be commenting publicly and talking about their employer. There are also serious legal consequences if employees use these sites and click on links to view objectionable, illicit or offensive content. An employer could be held liable for failing to protect employees from viewing such material. Apart from legal costs and fines, the damage to the organization's reputation could both be substantial.



### Thanks, but no thanks!

Businesses need to take stock of the situation and decide whether the risk of allowing people to use social networking sites at work is acceptable or not.

Businesses have three options:

1. Don't do anything,
2. Block everything (and that means Internet too), or
3. Be kind and let them use the Internet... but only when you want them to.

Today, most businesses opt for number 3 because it makes most business sense. You know your employees need the Internet to work. So blocking access is not really an option. Giving them total access to do what they want online is taking trust to the extreme. Yet having the ability to block or allow sites according to the business's needs is a solution that can and does work.

### Striking a balance

In today's networked world, it is impossible and stupid to isolate a business because of social networking sites. Despite the concerns, there are steps a business can take to allow social networking at the office and still maintain a level of control.

Here are a few pointers:

1. **Restrict access.** Allow access during their lunch break, before work starts and after work. This can easily be done using Internet monitoring and filtering software (and myriad other things).
2. **Educate and train staff.** Most employees are not aware of the time they spend on Facebook or that their actions online can cause security issues. Tell them in a language they understand how a simple click on a link they receive or an application they download can result in malware infecting their machine and the network. Additionally, tell them not to click on suspicious links and to pay attention when giving out personal details online.
3. **Set security and usage policies.** Have all employees sign any policies related to the use of the Internet at work, access to social networking sites and what they are allowed to say or do during office hours. Monitoring of all web activity is important and employees should be aware that their actions are being recorded and that failure to adhere to company policy can result in disciplinary action and/or dismissal.

### How GFI WebMonitor™ can help an organization

GFI WebMonitor, an award-winning solution currently being used by thousands of customers, gives organizations comprehensive control of the use of the Internet by employees in the workplace, performing both Internet monitoring and web security. It gives management the ability to monitor Internet browsing, block access to sites on an individual or group level, provide protection against hidden downloads as well as block and identify background processes that are downloading payloads which may be malicious in nature or use up network resources.



## Social networking at work: thanks, but no thanks?

GFI WebMonitor allows administrators to manage what sites users can browse and block access to websites in particular categories, such as adult material, online gaming, personal email, Peer-2-Peer, Facebook, MySpace, and more. Web monitoring is made easy with an extensive database that provides URL coverage and categorization for 205,000,000 domains and that is being continuously updated.

GFI WebMonitor also offers web security features that allow you to monitor what files employees are downloading, to block file-types such as MP3s and movies and to scan all files for viruses, spyware and malware using multiple antivirus engines. GFI WebMonitor lowers the risk of phishing by blocking access to phishing websites through the use of an auto-updatable database of phishing URLs. The web monitoring features also allow you to monitor and block Windows Live Messenger (MSN) chat sessions and file transfers.

GFI WebMonitor is also available as a dedicated plug-in for Microsoft ISA/TMG Server.

For information on GFI WebMonitor visit <http://www.gfi.com/webmonitor/>.

© 2010. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.