

Social Networking

– What Every Business Should Know

A ScanSafe White Paper May 2008

TABLE OF CONTENTS

	PAGE
TABLE OF CONTENTS	2
1.0 INTRODUCTION	3
2.0 THE GROWTH OF ON-LINE SOCIAL NETWORKS	3
3.0 BUSINESS BENEFITS OF SOCIAL NETWORKS	4
4.0 SOCIAL NETWORKING CHALLENGES	5
4.1 PRODUCTIVITY	5
4.2 SECURITY	5
4.3 LEGALITY AND COMPLIANCE	7
5.0 CAN WE JUST BAN IT?	8
6.0 ACCEPTABLE USE POLICY	9
7.0 ENFORCEMENT OF ACCEPTABLE USE POLICY	9
8.0 REAL-TIME SCANNING	10
8.1 SIGNATURE BASED DETECTION	10
8.2 HEURISTICS	10
8.3 CODE ANALYSIS	10
8.4 CODE REPUTATION	11
8.5 URL REPUTATION	11
8.6 TRAFFIC BEHAVIORAL ANALYSIS	11
9.0 SAAS WEB SECURITY	11
10.0 SUMMARY AND CONCLUSION	13
11.0 ABOUT SCANSAFE	13

1.0 INTRODUCTION

Unless you've recently returned from a very long vacation, you'll no doubt be aware that social networking can be defined simply as the on-line building of communities of people linked by various interests or activities. Examples include MySpace, LinkedIn, Bebo and the seemingly omnipresent Facebook. Social networks provide multiple ways for members to interact such as instant messaging, email, video and voice chat, file sharing, blogging and discussion groups. This multi-way flow of information is accomplished through Web 2.0 technologies, a collection of scripting languages and applications that have fundamentally changed the nature of the Internet from a one-to-many delivery device to a many-to-many global communication experience.

This paper addresses the nature and growth of on-line social networks and attempts to answer the following question:

How do organizations harness the considerable benefits made available by the existence of social networking websites, without incurring considerable risks to productivity, security and legality of operations?

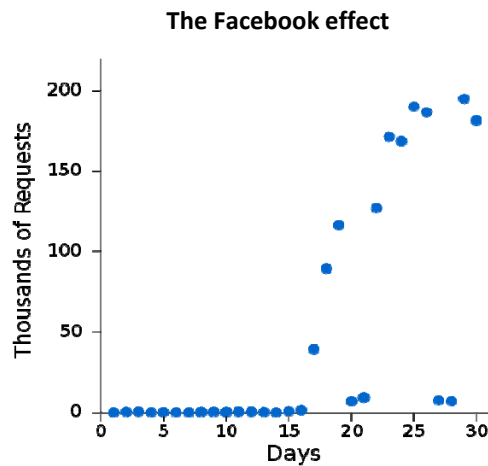
“How do organizations harness the considerable benefits made available by the existence of social networking websites, without incurring considerable risks to productivity, security and legality of operations?”

2.0 THE GROWTH OF ON-LINE SOCIAL NETWORKS

The speed at which social networking websites have gathered members is astonishing. Between July 2006 and July 2007 Facebook grew its overall user base by 270% and Bebo by 172%.¹ These figures disguise some real variation in the regional popularity of various social networking websites. Whilst MySpace and Facebook dominate the US market, Latin and South America primarily use Orkut, and Friendster dominates the AsiaPacific region. Whilst there is some evidence that the actual time that people spend on social networking sites may be levelling off, this could be interpreted simply as an indication of fierce competition between sites or, indeed, the fact that the astronomical rate of growth experienced through late 2006 and early 2007 was simply unsustainable. Whatever the reason, and with expansion into non-English speaking countries underway, social networks are not going away anytime soon.

“Between July 2006 and July 2007 Facebook grew its overall user base by 270% and Bebo by 172%.”

¹ Comscore, July 2007



To some extent, on-line social networking is no different from any other personal Internet use within the work place. Most organizations already have an Acceptable Use Policy (AUP) in place, communicate it clearly and consistently to staff, and enforce it with URL filtering capability of some sort. So why are social networking websites being treated differently? The answer lies in the vast amounts of personal information residing on these sites and their informal, dynamic nature.

3.0 BUSINESS BENEFITS OF SOCIAL NETWORKS

“A recent global survey by analysts IDC found that 38 percent of the respondents were using social networks to talk to customers, with 41 percent using them to communicate with co-workers.”

The symbiotic ideal of Web 2.0 and social networking that was no doubt foremost in the minds of its creators has been partially realised. Social networking in particular, has the potential to deliver great benefits to organizations and individuals alike. One example of such a site is LinkedIn. On this website individuals can research employment opportunities and be introduced to other professionals, whilst prospective employers can find the right candidates, describe the opportunities available in their organization and also search for partners.

Social networking tools are an excellent way of sharing ad hoc information – with employees, customers and business partners. The most forward-thinking organizations have understood the informal nature of social networks and used it to their advantage. Social networks can help to overcome the lack of togetherness that often afflicts a big, geographically distributed organization. Business ideas are often best discussed and developed within informal mediums.

The honesty often prompted by such informality can also improve the quality of customer feedback, increase brand awareness and enhance the provision of support. A recent global survey by analysts IDC found that 38 percent of the respondents were using social networks to talk to customers, with 41 percent using them to communicate with co-workers.

As a result of the adoption of social networking by business, the value of the social network application market is expected to increase from \$46.5 million in 2006 to a projected \$428.3 million by 2009. ²

² IDC The Business Value of Social Networking Applications, October 2007

4.0 SOCIAL NETWORKING CHALLENGES

Harnessing the power of on-line social networks for the corporate good remains a challenge in relation to the productivity of staff and the security and legality of operations. These are areas fundamental to the prosperity of any organization. Companies of all sizes are struggling to harness the more positive elements of social networking, without becoming one of its high profile casualties.

4.1 PRODUCTIVITY

The loss of working hours to the on-line social networking phenomenon has been well documented. One recent study estimated that 233 million working hours are consumed every month by social networking sites. The same study put a cost to UK businesses on this lost productivity of \$250 million every day.³ Another survey conducted at the beginning of 2008 put an annual figure of £6.5 billion on associated productivity losses.⁴

Social networking sites certainly seem to possess more addictive qualities than other personal websites. Keeping profiles up to date is indeed time consuming, and the long winded way of sending messages to other users of your network also takes more time than simply emailing that person in the first place. Perhaps the biggest part of the problem lies in the sheer amount of often irrelevant information that these websites contain. Looking at the average MySpace page, for example can feel like being swamped by trivia. There can't be many employers who haven't caught a staff member staring blankly at their monitor, not wanting to miss any changes to the relationship status of their friends or perhaps a change to their favourite films list.

People have used on-line tools to organize and expand their social lives for some time and it is arguable that this is not entirely to the detriment of their employers. However, the tidal wave of frankly irrelevant information unleashed by social networking websites is, for the most part, unwelcome to employers.

4.2 SECURITY

Employees accessing social networking websites in the workplace can have a profound impact on information security. The user defined nature of these sites means that it is now easier than it has ever been for cyber criminals to inject malware into unsuspecting sites. Malware is being inserted onto Web pages via insecure advertising servers, compromised hosting networks, straightforward user-contributed content, and even through third party widgets. In the past year there have been countless incidences of popular collaborative sites inadvertently hosting malware.

“One recent study estimated that 233 million working hours are consumed every month by social networking sites.”

“In the past year there have been countless incidences of popular collaborative sites inadvertently hosting malware.”

³ Peninsula, September 2007

⁴ GSS and Infosecurity Europe 2008, January 2008

Case Study – MySpace

An example of a popular social networking site hosting malware occurred last June when a fast-flux network, a disturbing advance in the development and use of bot networks, was used to spread malware via a flash movie on MySpace. Up to 100,000 MySpace accounts were affected by the attack. In effect, this MySpace attack was a double-whammy, combining the insecurities inherent in many Web 2.0 sites with a powerful, new and incredibly stealthy distribution technique. Unlike traditional 'bot' networks, fast flux networks abuse DNS to dynamically resolve an address to any number of infected PCs, as well as using the same technique to hide the control servers, which make them much harder to shut down. This ensures that the offending site(s) are active for a much longer period of time.

Using on-line social networks for business communication can be dangerous when you consider that these communications are not backed up, encrypted or stored in the way that usual business communications such as email would be. The security implications for organizations can be severe. If all information pertaining to a certain customer or transaction had to be produced for legal or regulatory reasons, the organization could be found wanting. Moreover, malware can be used to steal confidential data which could breach customer confidentiality and further regulations, as well as result in the organization incurring a serious financial penalty and losing its competitive advantage. Whether individual users accept and understand these risks is debatable, but their employers certainly should.

Case Study- Facebook

The BBC technology programme Click recently found that personal details of Facebook users could potentially be stolen through malicious programs masquerading as harmless applications. Facebook's response to Click was that users should employ the same precautions while downloading software from Facebook applications that they use when downloading software on their desktop. It should be evident to all and every Web user that just because a website is popular and trusted it does not mean that it is in full control of the nature of applications uploaded to it. The onus is on users to protect themselves. If those users are accessing Facebook from a corporate network then the owners of that network should take steps to protect it.

4.3 LEGALITY AND COMPLIANCE

The use of social networking websites can compromise the brand of an organization in other ways. The informality of such sites can seduce users into being considerably less careful about sharing opinions than they would be in conversation or even other electronic mediums such as email. Information confidential to the employer can easily make its way out into the public domain via the social networking medium. It's also very easy to make a throwaway derogatory comment about an employee, colleague or customer – and all too easy for that comment to be viewed by an altogether larger audience than the poster may have had in mind.

The implications of this loose talk for the employer are many. At one end of the scale an organization may suffer financial losses due to brand damage and loss of credibility. Furthermore, compliance with government or industry regulations relating to effective systems and processes for data control will almost certainly be prejudiced by the loss of information in this way. This may result in a substantial fine from the regulatory body for failure to manage confidential data with sufficient control or diligence.

Perhaps the worst case scenario is that of legal action being taken against the organization. Employees enjoying uncontrolled access to social networking sites could easily increase the likelihood of a successful claim against their employer for sexual harassment or unlawful sex discrimination. It is also worth remembering that compensation for sex discrimination remains uncapped in many jurisdictions.

The file sharing capabilities of social networks should also be a cause for concern for any CIO.

“It’s very easy to make a throwaway derogatory comment about an employee, colleague or customer – and all too easy for that comment to be viewed by an altogether larger audience than the poster may have had in mind.”

Case Study – IFPI

The International Federation of the Phonographic Industry (‘IFPI’) has sued over 6,000 individual file sharers in the UK, Austria, Denmark, Germany and Italy for copyright infringement. However, the IFPI has more recently started to take action against organisations rather than individuals, for example by writing to every university in Britain to point out the legal implications of unlicensed Internet copying (i.e. injunctions, damages, costs and possible criminal sanctions). In the United States, the Recording Industry and Association of America (‘RIAA’) sued an Arizona company because its employees were using the company’s resources to distribute copyrighted music. The claim was reportedly settled for \$1 million.

In reality, even if an employer is morally blameless, in practice they are more likely to be sued than a careless employee because they possess deeper pockets. They are more likely to be able to meet a substantial damages award, particularly as in most cases there will also be corporate insurance cover to meet such claims.

Even if a legal claim is unsuccessful, dealing with claims can make very substantial demands on management time and involve significant legal costs (which are often irrecoverable even if the defence is successful). In addition, the mere bringing of a claim can give rise to undesirable adverse publicity, creating pressure on the business to settle claims even if they are without merit.

5.0 CAN WE JUST BAN IT?

“Banning social networking sites is unlikely to be effective.”

The level of risk posed by social networking websites is proving unacceptable to many organizations. This is leading to increasing numbers of companies simply blocking them. A survey last Autumn showed that the proportion of organizations that have a blanket ban on employee access to social networking sites has jumped from 18% to 33%. MySpace, YouTube and Facebook the sites companies most likely to be blocked. LinkedIn comes fourth in the 'most blocked' list.⁵

If an organization feels that social networks have nothing to offer except lost productivity and a huge security headache it is, of course, perfectly entitled to ban access to them. The same legal principles apply to employees accessing social networking websites as any other, so provided that the AUP is communicated to all employees that should be the end of the matter.

If only life were that simple. The fact is that banning social networking sites is unlikely to be effective. This is partly because the nature of such websites is changing. As mentioned above, the main websites are seeing a leveling off in new users and the amount of time actually spent on each visit. Instead huge numbers of specialist, niche social network sites are springing up to cater for very specific interests. It is debatable how these sites would be classified by a URL filtering engine and whether they would be classified correctly. There would certainly be a delay in the classification because all URL filters take time to crawl the Web and classify new content.

“Generation “Y” has come of age using social networking tools and expects them to be available in the work place.”

Human nature and history suggest that if something is prohibited, people just find new ways of acquiring the banned resource. In the case of social networks, employees are starting to access them on mobile phones instead of their PC or laptop. An employee accessing a social network site in this manner wastes more time and is subject to less control than if they enjoyed controlled access from within the corporate network.

Banning social networking websites from within the workplace also alienates younger employees. Generation “Y” has come of age using social networking tools and expects them to be available in the work place. The balance of working and personal lives is a subject that continues to enjoy a very high political and media profile, and social networks allow employees to manage some of their personal lives from their workplace, perhaps in a more efficient manner than would otherwise be the case. The fact is that the current generation is demanding more flexibility in their working arrangements, and banning social networking flies in the face of this culture. If your staff work long hours, refusing to allow them half an hour to arrange their weekend social life for example can seem a little churlish. Preventing staff having access to social networks at all will almost certainly have a negative effect on staff retention.

“Preventing staff having access to social networks at all will almost certainly have a negative effect on staff retention.”

As new technologies have emerged, the instinct of many organizations has been to try to ban them. Internet access on every PC and Instant Messenger are two examples of technology that was initially treated with suspicion and often an instinct to block or prevent access. However, employers soon realised that these concepts could bring great benefits for business as well as presenting risks, so the smart ones adapted and found ways to harness the good and mitigate the

⁵ ScanSafe, September 2007

bad. Social networking websites should be treated in the same manner. Trying to stop people accessing them is like trying to put toothpaste back into a tube.

With technology such as Instant Messenger the novelty also wore off fairly fast. Initially, some more work-shy employees might have thought it was great that they could spend hours chatting to friends uncensored, but generally people have moved to use it more as a work tool with personal chat time reducing. The same already seems to be happening with social networking sites. Perhaps the novelty is wearing off already and people are ready to use it more constructively. Banning it now would therefore be counter-productive.

6.0 ACCEPTABLE USE POLICY

If prohibiting the use of social networking websites in the workplace is not a realistic option for employers, controlling them certainly should be. Despite the benefits that can be realised from the existence of such tools, they still expose organizations to an unacceptably high level of risk.

The first step towards mitigating this risk is by making absolutely clear to employees the conduct expected of them whilst on-line. In particular, employees should be aware that posting remarks to sites about their employer, mentioning the employer by name or claiming to represent the employer's opinion is expressly prohibited. Posting pictures of yourself in any company uniform or with company logos visible should also be prohibited. The organizations should also set out its policy on whether employees should communicate with customers via this forum. All of this can be contained within a corporate AUP to which all employees should be signed up. The AUP should be regularly reviewed and updated and should be easily accessible to staff. Monitoring on-line behaviour is acceptable provided that employees are made aware that their Web use is subject to such controls.

Depending on the size and culture of an organization, staff may benefit from some training on the implications of posting on social networking websites both in terms of their professional and personal lives. If staff realise that a carelessly placed remark or picture could cost them their livelihood they might be a little more careful about what they upload.

“The first step towards mitigating this risk is by making absolutely clear to employees the conduct expected of them whilst on-line. ”

7.0 ENFORCEMENT OF ACCEPTABLE USE POLICY

The drawing up and communication of an Internet Acceptable Use Policy is a waste of time unless it is also enforced. This is usually achieved with the deployment of URL filtering software or services. These consist of databases, which are built as URL filtering vendors crawl the Internet, categorizing every site that is found. Most databases now contain a social networking or chat category and specific URLs can also be blocked as can downloads of certain file types or MIME types. Organizations can also use these services to limit visits to social networking websites, for example to between 12pm and 2pm or outside of the working day altogether. An alternative approach is to simply issue a quota for Web surfing as a whole. Once an employee has used up their one hour quota for example, that's it for the day.

The use of URL filtering software or services is a good first step to mitigating the risk posed by social networking sites but it is not a complete solution. Whilst it certainly goes some way to

“The use of URL filtering software or services is a good first step to mitigating the risk posed by social networking sites but it is not a complete solution.”

alleviating the productivity and legal risks posed by social networking, it only goes a little way towards addressing the security concerns.

URL filtering can only be as effective as its database of categorized websites. With social networking websites popping up on the Web at an unprecedented rate and covering all sorts of obscure interests, this approach alone is not enough. Given that no Web crawler can cover all of the Web all of the time, the information being used to categorize a site is likely to be at least a few hours old.

The bigger problem, however, concerns malware. Category-based filtering alone will not prevent users becoming infected with malware. There is only one way to enforce your corporate AUP *and* protect your network from the malware lurking on social networking websites. This is to ensure that in addition to all Web requests being checked against a categorization database, all of your Web traffic is scanned in real-time.

8.0 REAL-TIME SCANNING

“Real-time scanning means that all content on a URL is scanned immediately, every time that it is requested.”

Real-time scanning means that all content on a URL is scanned immediately, every time that it is requested. This is an important distinction from URL filtering which merely filters URLs and compares them to a limited database of known categorized URLs. Effective real-time scanning should be powered by a combination of multiple detection technologies. When used on their own to combat malware (as they are by many Web security vendors), these technologies can often fall short. However, when these techniques are combined in a cocktail approach, their strengths are leveraged and their shortcomings mitigated. These techniques are as follows:

8.1 SIGNATURE BASED DETECTION

Signature-based engines are extremely effective at identifying and blocking known threats. Multiple signature-based engines form an important part of a multi-layered cocktail approach to real-time scanning. However, signature-based malware detection only works for known malware. It is not useful for new threats. Additionally, in order to be effective signatures must be delivered and propagated quickly, which is a time-consuming task.

8.2 HEURISTICS

Using a rule of thumb to detect *variants* of known malware is an effective tool in the fight against malware. However, if your heuristics are too aggressive, you experience false positives. Also, heuristics are designed to increase the probability of detecting something that is similar to something that you have seen before. This means that a heuristic won't detect completely novel malware.

8.3 CODE ANALYSIS

The behavior of code can be determined by modelling program logic, behavioral rules, and contextual system call analysis techniques that suggest good or bad intentions.

8.4 CODE REPUTATION

Unlike URLs whose content can change, a binary can, in fact, have a reputation based on historical analysis. “Good” code can be treated differently to unknown or “bad” code.

8.5 URL REPUTATION

URL reputation is derived by examining parameters such as IP address information, country of the Web server, history and age of the URL, domain registration information, network owner information, URL categorization information, and types of content present. URL reputation provides a “credit history” of sorts for a URL, but it does not provide current information about the safety of a URL. When looking at Web safety, it is useful to bear in mind that past performance does not predict future performance. As we’ve seen, “good” websites today may host malware tomorrow.

8.6 TRAFFIC BEHAVIORAL ANALYSIS

Traffic behavior analysis identifies suspicious, atypical traffic which would suggest, for example, a new phishing scam or perhaps active malware communications from an infected notebook computer to a command-and-control computer. Unlike reputation techniques, which are based on past behavior and provide valuable historical context, actively monitoring Web traffic patterns and anomalies provides a real-time look into emerging threats. The important point to note here is that behavioral analysis of traffic is only effective if it is based on a large volume of real world traffic.

A combination of URL filtering and real-time scanning of Web traffic is the most efficient way of allowing employees the freedom to use social networking sites and harnessing their more positive elements. Unfortunately, the only way to provide Web security of this calibre in-house would be to deploy multiple layers of software. We have established that URL filtering software is not up to this challenge. Although deploying it on a dedicated gateway appliance alongside gateway anti-virus [and desktop anti-virus] protection suites might mitigate some of the security threats posed by social networking sites, it simply doesn’t tick all of the boxes. Furthermore, these numerous products would be expensive and time consuming to integrate and manage. Inefficiencies would persist because although these products might be the leaders in their particular field they cannot communicate with each other.

“A combination of URL filtering and real-time scanning of Web traffic is the most efficient way of allowing employees the freedom to use social networking sites and harnessing their more positive elements.”

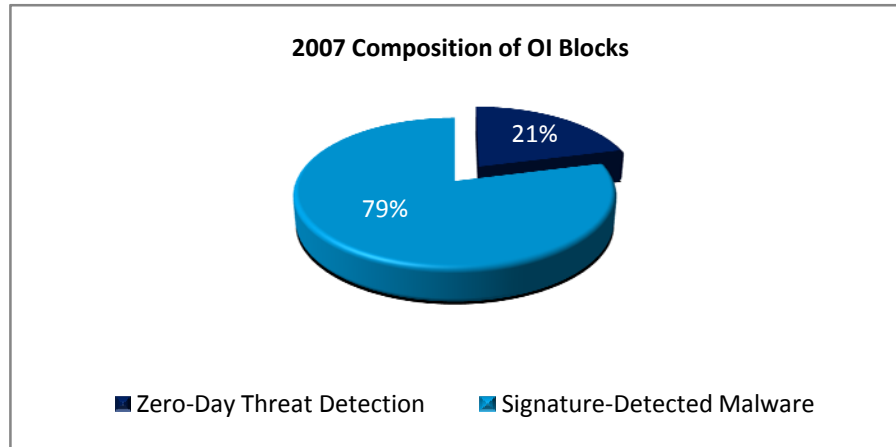
9.0 SaaS WEB SECURITY

ScanSafe is the pioneer and global leader in the provision of Software-as-a-Service (‘SaaS’) Web Security. Our award winning service protects organizations of all sizes from Web based malware attacks and enables safe, productive use of the Web without incurring up-front capital, hardware or management costs.

ScanSafe’s Web security services are built on Outbreak Intelligence™ (‘OI’), a proprietary security platform that detects new and known malware threats. By leveraging its unique position at the internet level and processing several terabytes of Web data each day, OI has unmatched visibility of global Web data to proactively identify zero-hour malware threats. OI uses multiple signature-

“ScanSafe’s Web security services are built on Outbreak Intelligence™ (‘OI’), a proprietary security platform that detects new and known malware threats.”

based anti-malware scanning engines, multiple reputation and behavior-detection engines, and heuristics detect new malware and avoid false positives. This combination of multiple, correlated detection technologies and the industry's largest Web data set make OI the most effective solution against new Web malware attacks.



Customers of ScanSafe receive a 360° view of the current Web threat environment compared to the very limited view given by those utilizing URL filtering alone. This is the difference between seeing the full picture and just one piece of the puzzle. This 360° degree view of Web threats that ScanSafe delivers allows the various, traditionally disparate, components of Web security to be connected.

“The adoption of SaaS Web Security brings many benefits for an organizations looking to manage and control the use of on-line social networking.”

The ScanSafe service is implemented via a simple configuration change which routes organizations Internet traffic through ScanSafe’s global network of datacenters. Web requests are filtered in the Internet ‘cloud’ and malware is removed before serving clean traffic back to the user. The corporate AUP can be applied to all users regardless of location and management is also simplified because no endpoint updating is required.

The adoption of SaaS Web Security brings many benefits for an organizations looking to manage and control the use of on-line social networking. These benefits allow an enterprise to “work smart” by focusing their energies on activities core to their business. Precious IT resource can concentrate on strategic activities such as setting up social networks for staff and customers. They can contribute to their organization’s bottom line rather than spending large amounts of their time fire-fighting the results of uncontrolled access. Service Level Agreements concerning up-time, latency, false positives and negatives are standard and SaaS Web Security is fully scalable. As the social networking and Web threat landscape shift, organizations can plan capacity and budget with confidence. In summary, the adoption of SaaS Web Security allows IT resource to *innovate* rather than *maintain*.

10.0 SUMMARY AND CONCLUSION

The conclusions reached by this paper are as follows:

- On-line social networks such as Facebook, MySpace and Bebo have grown at an astonishing rate with nearly 108 million users of such networks being forecast by 2012
- Social networks can bring great benefits to business in areas such as recruitment, creative activity and customer support
- Social networking can also exert a serious drain on workplace productivity with estimates of 233 million working hours a month being lost
- Social networks also pose significant security issues both in terms of operational information not being encrypted or backed up and also malware being injected into such websites
- Legality and compliance with industry or government regulations can also be affected when information confidential to the employer is posted in the public domain – a task made all too easy by the existence of social networking websites
- Whilst organizations are legally free to do so, banning social networking websites in the work place is likely to be both ineffective and counter-productive
- Allowing staff controlled, regulated access to social networks is the best balance and expected conduct should be communicated via an Internet Acceptable Use Policy
- This policy should be enforced by a mixture of URL filtering software or services and real-time scanning of all Web traffic
- SaaS Web Security is usually the most cost-effective way to realise the benefits of social networking whilst keeping it productive and safe

11.0 ABOUT SCANSAFE

ScanSafe is the largest global provider of Web Security-as-a-Service, ensuring a safe and productive Internet environment for businesses. ScanSafe solutions keep viruses and spyware off corporate networks and allow businesses to control and secure the use of the Web and instant messaging. As a SaaS solution, ScanSafe's services require no hardware, upfront capital costs or maintenance and provide unparalleled real-time threat protection. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe scans more than 20 billion Web requests and blocks 200 million threats each month for customers in over 80 countries.

With offices in London and San Francisco, California, ScanSafe is privately owned and financed by Benchmark Capital and Scale Venture Partners. The company received the CNET UK Business and Technology award for Security Product of the Year 2008, a 2007 CODiE award for Best Software as a Service Solution, the 2008 and 2007 SC Magazine Europe Award for Best Content Security Solution and was named one of Red Herring's Top 100 Technology companies. For more information, visit www.scansafe.com.

SOCIAL NETWORKING – WHAT EVERY BUSINESS SHOULD KNOW

Contact ScanSafe

ScanSafe US
185 Berry Street
San Francisco, CA 94107
T: 415 692 2000
F: 415 536 5949
E: info@scansafe.com

ScanSafe EMEA

The Connection, 198 High Holborn
London WC1V 7BD
T: 020 7959 0630
F: 020 7959 0631

About ScanSafe

Founded in 1999, ScanSafe is the leading global provider of Web Security-as-a-Service, ensuring a safe and productive Internet environment for businesses. As a SaaS solution, ScanSafe's services require no hardware, upfront capital costs or maintenance and provide unparalleled real-time threat protection. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe scans more than 20 billion Web requests and blocks 200 million threats each month for customers in over 80 countries.

For more information visit www.scansafe.com