SOPHOS

Social media in the enterprise: Great opportunities, great security risks

Just as consumerization drove the iPhone's rapid growth from a consumer device to an enterprise business tool, social media, too, is being embraced as an indispensable business tool. However, as social media is organically adopted for a growing array of uses, are its security challenges receiving the necessary scrutiny? This white paper examines the transformative business effects of this technology, explores its evolution and presents ways businesses can realize its full benefits while avoiding potentially serious pitfalls.

A Sophos white paper

June 2010

Social media in the enterprise: Great opportunities, great security risks

Social media arrives as an enterprise tool

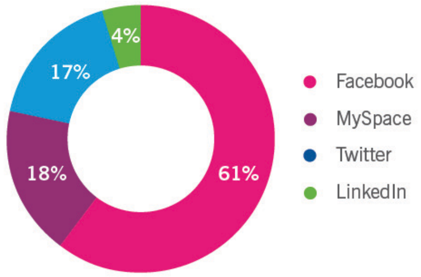
Initially, social media use within enterprises was seen as a distraction, a timewaster and a business drain as employees used work PCs and business time to update their personal Facebook accounts and stay up to date with their peers' activities. Over time, some organizations became concerned about the loss of productivity; and because of this threat, some even started blocking social networking sites.

For others, simply imposing a blanket block was impractical. These organizations understood that banning these sites could pose a greater risk as some users would find ways to circumvent the ban to access these applications. These organizations also see value in social media sites and use it for quick updates among work groups, with tags and postings effectively replacing the traditional, more formal corporate communications infrastructure. Many enterprises are aggressively driving this shift to bring velocity and openness to communications, and many organizations are adopting it.

Salesforce.com has pulled Facebook profiles into its CRM offerings. LinkedIn has been plugged into Lotus Notes, providing direct integration with email. Twitter is broadly integrated into a variety of dashboards commonly used in the enterprise. Facebook alone boasts more than 700,000 business accounts. The web app/thick app mashups (combining two or more applications together to create a new derivative) have begun, and with them comes a whole new world of opportunity and an interesting challenge in managing security. However, with such large and widely used applications starting this integration, enterprise use is bound to accelerate further.

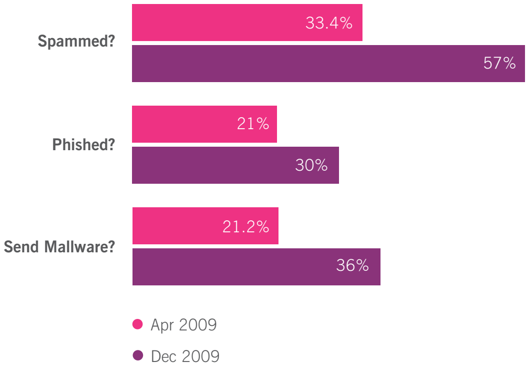
Securing enterprise social media

Given its origins, enterprise users might have concerns about security when deploying social media. According to a Sophos survey conducted in December 2009, 60% of respondents believe that Facebook presents the biggest security risk of the social networking sites, significantly ahead of MySpace, Twitter and LinkedIn.

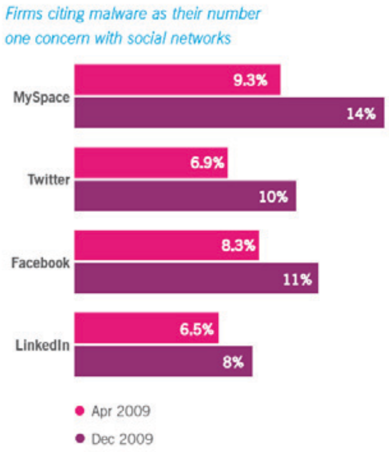


Which social network do you think poses the biggest risk to security?

This survey also cited a 70% rise in the proportion of firms that report encountering spam and malware attacks via social networks during 2009. More than half of all companies surveyed said they had received spam via social networking sites, and over a third said they had received malware.



Furthermore, more than 72% of firms believe that employees' behavior on social networking sites could endanger their business's security—an increase from 66% in the previous study. The number of businesses that were targets for spam, phishing and malware via social networking sites increased dramatically, with spam showing the sharpest rise from 33.4% in April to 57% in December (Source: Sophos Security Threat Report: 2010).



This shows that malware authors and hackers go wherever there is a captive audience. It is the real-time, rich nature of these applications that attracts individuals, enterprises and hackers. As with other online activities, malware and hacking on social media sites raise the risks of social engineering—getting users to run a program they should not, participate in a fake scheme or provide personally identifiable information. Social media platforms are by their very nature a target for malicious activity; they provide direct access to victims in a rich, relatively open environment.

Because of this, social media providers and users must be vigilant about security as they work to make it a sustainable and useful tool:

1. Familiarize yourself with your organization's social media policy so you don't inadvertently break the rules.

2. Choose sensible, strong, hard-to-guess passwords. Use at least 14 characters and mix in upper- and lowercase letters, numbers and symbols.

3. Social networking sites are, by design, dependent on a large number of users. Always review default settings and avoid providing personal information such as your date of birth, mobile numbers and travel plans whenever possible.

4. Do not post images, pictures or information that might embarrass you, your company or your customers.

5. Avoid treating social networking sites as personal diaries. Assume that everyone including your boss, your family, your friends and your enemies can read whatever you post.

6. Malware authors, spammers and phishers are increasingly active on social networking sites, and their methods are not always obvious. Be sure to visit these sites from a fully protected computer or device.

7. Never click on links just because you know the sender; malware will infect a user and then automatically fire itself out under their name to all their contacts.

8. Be wary of spammers trying to connect with you by sending invitations. If you don't know the sender, the best thing to do is ignore the request.

Social networks need to be more proactive regarding security to ensure users are safe and are not misusing functionality. They should:

1. Regularly and diligently scan links, content and messages that are shared between users. Doing so will help determine if they are, for example, spam, malware or a phishing scam.

2. Educate users about the attacks that can happen online, and provide security awareness pages that help alert users to the latest threats.

3. Enforce the use of sensible non-dictionary passwords.

4. Block repeated attempts to guess passwords by increasing delay time. Doing so will prevent brute-force attacks against passwords.

Future social media capabilities to proliferate use

Social media also is transforming common business functions, including:

- **Authentication:** Today's social media platforms feature data and application controls, which users should follow to ensure appropriate security. In a world where services are increasingly accessible via standard APIs, permissions and authentication should be a critical requirement, but at this point they are not.

- **Identity:** Identity is often considered to be synonymous with authentication—but identity is more than just a username and password. Many social media sites share this personal identifying information with the entire social networking community.

- **Contacts:** No longer just an address book in your PC or a few saved numbers on a phone, this is now a portable list of everyone you regularly communicate with, organized according to the various business groups you belong to. It's similar to how you may group your list of friends by common interests, activities or locations.

- **Activities:** Activities are similar to your personal interests, but with more of a business slant. These include your preferred information sources, whom you contact regularly and what you read.

Standards for sharing contacts, activities and other data types are currently in development. Although this holds promise for improved applications control, it also challenges organizations to develop a business model that affords users the ability to use these sites while protecting their personally identifiable information. So the question remains, how do organizations create these models?

The industry has done a great deal of work in this area, and more is needed to deliver consistent, trustworthy enterprise use. Enterprise security policies and global data protection policies should be reviewed, refreshed and monitored consistently to keep pace with evolving technology. Social media providers must make education a priority and keep users up to date on the potential risks associated with social networking use. Most importantly, a set of standards and tools must be developed to help rein in potential threats and keep social networking users out of harm's way.

At Sophos, we've focused on the importance of simplicity and enablement. Although an invisible security product sounds unusual, it is consistent with our goal of avoiding user disruption. As for social media, the benefits are there, enterprises are willing—and someone needs to take a visible stance. Even more fundamentally, we all need to explore the vast implications of flexibility versus security in our hugely connected world.

Conclusion

Social media is evolving at breakneck speed. There are huge benefits to be realized from the use of these technologies in the enterprise, such as enabling better collaboration and networking than ever before. These technologies will result in greater connectivity, greater integration and greater value through collaboration.

Enterprises should expect strong integration of social media in their environments, both as a tool to talk to the world and through direct integration with corporate applications. Consumerization could drive such technology in the enterprise organically, without recognition by the security staff. Planning for such integration and being ready to manage the process of adoption with risk management is critical. The most significant risk is usually the unplanned, mass-adopted behavior or technology change.

Boston, USA | Oxford, UK

SOPHOS
WWW.SOPHOS.COM