Social Networking Is a Must

Social networking is fundamentally shifting the way we interact, communicate, organize, form opinions, and even shop; it's blurring boundaries, increasing transparency and creating fluidity in everything we do. Linking a twelfth of society and growing rapidly, companies, large and small, can no longer ignore or try to block social networking in their environment. It's a part of the fabric in which we now learn, play and work.

The reality is you need to go where your target audiences are – and people are more likely to participate in a social media forum than any other venue. Customers, partners, and employees, alike expect to engage with you via social media – it's a way for you to stay connected, gather feedback, recruit, and collaborate. As a result, you need to support social media in your environment to enable the innovation, increased productivity, and accelerated growth that will drive your business.

Social Networking Risks

All the things that make social media so attractive to users – the personalization, the ease with which information can be shared, and the real-time nature of the medium – pose significant risks to your business. The following are the top four risks you face when you use social networking:

1. **Malware:** In 2010, social media became the preferred communications vehicle for users, who are spending more than 700 billion minutes per month on Facebook alone, making social networking sites and their users ideal malware targets. According to Sophos, 40% of users were infected by malware from social networking sites. Typical attacks draw on the trust relationship established between users and their connections. They try to trick users into giving up information and access that can be exploited for financial gain. Some examples of malware particularly successful in social media are:

   Phishing: With increasingly sophisticated techniques, attackers pose as one of your legitimate social networking connections and try to lure you into providing sensitive information, such as your login credentials. They prey on the tendency of most people to use the same passwords for all their accounts, hoping that by tricking you into giving one username and password they can get access to more profitable banking, financial and other online accounts.

   Most users have their radar ON concerning financial accounts, but their daily login to a social networking site is just a speed bump, creating an opening for cybercriminals to steal online assets. This is why more and more phishing attacks are targeting seemingly "non-relevant" online user accounts.

   Click-jacking: Attackers lure you into clicking on a link, perhaps posting it on your wall and then spamming your friends to "check it out," or "view my photos." When someone clicks on the link, they unwittingly install malware (code or script) that can be used to steal information or take control over their computer. Click-jacking uses the dynamic nature of social networking and a willingness to click on links from those you know, and even those you don't, to quickly reach a large audience, cajole you into revealing private information (e.g. through surveys), collect hits for ad revenue, and eventually allow access to your entire social network.

2. **Data Loss:** Social networking is about making connections and sharing experiences and information, however, sometimes that information is not meant to be made public. It's not uncommon for people to inadvertently post confidential information – "hey, I just met with xxx and I think I am about to make a huge commission," or "I'm pulling my hair out, if we can't fix this software bug soon, I don't know that I will ever sleep again," that provides "insider knowledge." There have also been cases in which employees have unintentionally posted proprietary software code to social networking sites, exposing sensitive intellectual property. These actions, though unintentional, can potentially violate industry-specific regulations, impact your reputation, or put you at a competitive disadvantage.

3. **Bandwidth Consumption:** As much as 40% of employees report that they are on social networking sites at work, creating a potential strain on bandwidth to the detriment of other business applications. Last year, when the U.S. government mandated open access to social networks, traffic on the network increased by 25%. Video alone (think of all the videos your friends share and you link to through Facebook or Twitter), can overwhelm many networks. A single video stream usually consumes between 500k to 1.2 Mbps (and that's not even HD, which can be up to 4 to 7 Mbps), and when you have tens or hundreds of people accessing videos it's easy to see how overall performance can degrade.
4. **Productivity Loss:** Social networking sites are becoming online destinations, enabling you to post and read messages, date, shop, upload or check out videos, and play games. This makes them increasingly convenient and engaging for users, drawing them to spend more and more time there, as well as increasingly challenging for the business to appropriately control. When unchecked, the time spent on social networking sites can affect productivity, as your employees spend more and more time (think back on the 700 billion minutes on Facebook) playing Farmville during business hours.

Requirements

While you find yourself compelled to allow social media to compete and thrive in today's global economy, you do not need to expose your business to undue risk. There are ways to protect against and mitigate the risks posed by social networking. Specifically, your solution needs to provide:

-> **A Real-Time Web Defense** – social networking is constantly changing, as are the tactics used by attackers to exploit it. As a result, your solution needs to analyze your web traffic on the fly and uncover threats that may be hidden there. Real-time analysis of dynamically changing links provides risk analysis and timely protection to keep social media safe. So when you see "hey you should take a look at this," you can either allow or deny based on the potential risk it poses.

-> **Selective Social Networking Controls** – to protect against data loss and comply with industry-specific regulations, you need to be able to manage the actions your employees can take within social networking sites. For example, you may want to prevent employees from uploading attachments, photos or video to social media sites, thereby preventing risks of inadvertent data loss or risks to your corporate reputation. The key is to have granular control over what can be done within social networking. This requires a solution that not only looks at where the initial traffic is coming from (e.g. Facebook, YouTube, etc.), but also at what is being done within that application (email, posting messages, downloading attachments).

-> **Caching** – you can't allow social media to overrun your network and adversely impact business critical applications, however, because social networking is becoming so integral to business, you cannot simply block it. What you can do is offset any potential performance degradation with caching, which allows you to locally store data and video files after an initial download and make them readily available to users who want to subsequently access them. In this way, you can enable access to social networking without compromising the performance of other traffic on the network.

-> **Policy Flexibility** – to manage productivity, you need to be able to set acceptable use policies within social media. You may choose, for instance, to block access to Farmville during work hours; or if you allow it, you may want to give it a lower priority, so it doesn't impact business critical applications. With a flexible policy framework, you can prioritize and manage the activities that are allowed or disallowed, and when. The ability to delineate between social networking sites and specific applications or content within those sites is crucial to setting an effective acceptable use policy. So, if you elect to block games, you can block both standalone games, as well as games within social media sites.

Blue Coat Web Security solutions help you achieve the level of protection, performance and control you need over social media to allow you to take advantage of its benefits. For information on the specifics of the Blue Coat Web Security solutions, please visit us at www.bluecoat.com/products.

Blue Coat Systems, Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA USA // +1.408.220.2200

EMEA Headquarters
Hampshire, UK // +44.1252.554600

APAC Headquarters
Hong Kong // +852.3476.1000