



Likes, Links, and Lessons Learned

A TrendLabs Primer

5

Things Every Small Business Should Know About Social Networking

From the biggest media moguls to the most humble convenience stores, businesses are establishing their presence online to reach their customers in the fastest and most cost-effective way. This is the social networking phenomenon and it is here to stay. But did you know that social networking can be risky to businesses, regardless of size?

FACT 1

Businesses of every size and type are adopting social media.

Large enterprises are not the only ones getting their own slices of the social media pie; small businesses are, too. A 2010 U.S. National Small Business Association (NSBA) study reported that 47% of their small business respondents used social media for networking purposes.¹

LinkedIn ranked first in their list of most utilized social networking sites, closely followed by *Facebook*. It's not hard to see why, as all they need to engage in what is essentially free advertising is a computer and Internet access.

An audience to capture exists as well, as according to a 2010 Nielsen study, close to three-quarters of the world's Internet population (74%) visit social networking sites or blogs and spend an average of almost six hours per month on social media sites.²

As a very cost-effective means to bring public attention to a product or to a service, social media are no doubt very powerful and popular business networking tools and will continue to be so in the years to come.

Source: NSBA, 2010

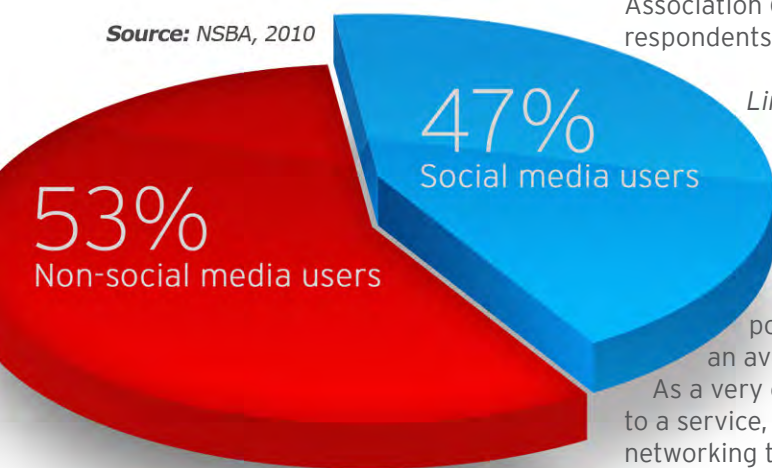


FIGURE 1. RATIO OF SMALL BUSINESS SOCIAL MEDIA USERS TO NON-USERS

¹ http://www.nsba.biz/docs/nsba_2010_technology_survey.pdf

² <http://blog.nielsen.com/nielsenwire/global/social-media-dominates-asia-pacific-internet-usage/>

FACT

2

More and more people access social networking sites at work.

The Ponemon Institute, in a recent global survey on social media risks, found that most IT security professionals agree that the use of social media in the workplace is important to achieving business objectives.³ This is not exactly alarming news, as the social networking phenomenon is affecting the entire world. In fact, a Trend Micro corporate end-user survey of 1,600 respondents from the United States, the United Kingdom, Germany, and Japan found that 24% of employees indulged in social networking at work in 2010, up from 19% in 2008.⁴

The same Ponemon Institute study also found that users engaged in social networking at work for both business and nonbusiness reasons. In fact, 60% of the employees surveyed used social media for at least 30 minutes per day for personal reasons. Users from the United States, the United Kingdom, France, Italy, and Mexico posted the highest social media usage rates for nonbusiness reasons. Organizations in Germany, on the other hand, posted the highest social media usage rate for business purposes.



FACT

3

Even small businesses are fair game when it comes to social networking threats.

Small businesses should realize that despite their size, they are not immune to social media threats. In fact, being taken advantage of by cybercriminals is an all-too-real possibility.

Take, for example, a malicious *Facebook* and *LinkedIn* incident Trend Micro engineers discovered last July.⁵ This particular attack made use of a *Facebook* wall post with the subject, "The Video That Just Ended Justin Biebers Career For Good!" The enticing subject matter may have lured users to click the malicious link to a *LinkedIn* page. Users were redirected to a page that had a video-player-like interface asking them to answer a survey before they could play the video. Answering the survey, however, did not allow them to watch the video; the video did not even exist.



Apart from being tricked into answering a survey for a nonexistent reward, users could have also suffered more serious consequences. The cybercriminals behind the attack, for instance, could have easily appended a rogue antivirus software or other malware as payload, putting affected users and their organizations at greater risk.

Employees don't necessarily have to access social networking sites to fall prey to social media attacks. A similar attack in April led spam recipients who were duped into believing their *Facebook* passwords were unsafe to open a malicious file attachment and to install malware in their systems.⁶

⁵ <http://blog.trendmicro.com/facebook-attack-leverages-linkedin/>

⁶ <http://blog.trendmicro.com/facebook-events-credits-and-passwords-being-used-for-attacks/>

FACT

4

Cybercriminals can use social media to gather sensitive information about companies and their employees.

As previously stated, more and more employees are accessing social networking sites at work. The fact that businesses of every size, including small ones, use social media in order to communicate with their customers and prospects is not escaping cybercriminals' attention as well.

By simply keeping track of the social networking habits of a company and its employees, cybercriminals can easily gather information the organization want to keep under wraps.⁷ Scouring tweets, blog entries, and status updates of careless employees can also inadvertently expose company secrets such as the identities of key personnel and even its financial status and internal problems.

A 2009 Deloitte study also revealed that 27% of the employees surveyed did not consider the ethical consequences of posting comments, photos, or videos online.⁸ Unless certain steps are taken, a company's employees could be revealing confidential data to just about anyone, including cybercriminals, with the simple act of posting status updates.

FACT

5

Social networking at work should be regulated to safeguard your business from attacks.

Social networking exposes small businesses to unique vulnerabilities. As a result, unique measures must be taken to safeguard critical business data from exploitation. Organizations must formulate formal policies on social media use in the workplace, regardless of business size.

Formulating policies is, however, not enough; strictly enforcing them is crucial, too. Employees should be informed of best social networking practices,⁹ along with potential consequences of abuse.

Guidelines must be set; these must be clear and concise so there is no room left for doubt or error. Keep in mind that even a tiny slip-up on any social networking site not only makes a business vulnerable to attacks but can also lead to reputational damage.

⁷ <http://about-threats.trendmicro.com/RelatedThreats.aspx?language=us&name=Anatomy+of+a+Data+Breach>

⁸ http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_2009_ethics_workplace_survey_220509.pdf

⁹ <http://about-threats.trendmicro.com/ebooks/socialmedia-101/#/1/>

How can you protect your business?

Social networks such as *Facebook*, *Twitter*, and *LinkedIn* are here to stay. The best thing you can do to protect your business is to empower your employees with best practices and guidelines to minimize risks of using social media:

- **Monitor employees' social networking usage.** The previously mentioned Ponemon Institute study found that over half of the employees surveyed browsed nonwork-related sites, including social networking sites, while at work. Studies also showed that employee productivity has gone down due to social media use. Control your employees' Internet usage with [*Trend Micro™ Worry-Free™ Business Security*](#), which protects your network from employees who surf inappropriate websites and from the download of malicious files. It also monitors your employees' Internet usage on specified hours or days.
- **Provide easy-to-follow guidelines.** Regardless of whether or not social networking is permitted at work, employees need to know what information they can post about your organization and who can post what information. Keep the following in mind when creating your organization's social media guidelines:
 - To stay within ethical guidelines, remind your employees that they are employed or paid by your company.
 - Remind customers to only share personal information via email or personal messages. Let them know where to go for help if they have questions that involve revealing confidential information.
 - Use resources such as [*SocialMedia.org*](#)¹⁰ to develop your guidelines and to learn more about social media.
- **Be social but be smart.** Only publish information that you feel perfectly comfortable with disseminating widely, depending on your business goals. Limit the amount of personal information your employees share online as well. Finally, remind employees to avoid clicking suspicious links shared by people they do not know.
- **Define what's confidential.** In your security policy¹¹, cover social networking sites such as *Facebook*, *Twitter*, *LinkedIn*, and more in your nondisclosure agreement for confidential business information.



¹⁰ <http://www.socialmedia.org/blogwell/>

¹¹ http://us.trendmicro.com/us/trendwatch/core-technologies/competitive-benchmarks/index.html?cm_re=HP:Acc:1- -CORP- -SPN+Benchmarks

For more information on the threats featured in this primer, please refer to our materials in the following portals:

- [Threat Encyclopedia](#): Our malware, spam, malicious URL, and Web attack entries such as "[Spam, Scams, and Other Social Media Threats](#)" provide more information on how cybercriminals use social networks to infect users' systems and to infiltrate corporate networks.

- [TrendLabs Malware Blog](#): Our blog entries like "[The Geography of Social Media Threats](#)" provide more information on the latest developments in the social media threat landscape.



ABOUT TRENDLABSSM

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to:

- Continuously monitor the threat landscape across the globe
- Deliver real-time data to detect, to preempt, and to eliminate threats
- Research and analyze technologies to combat new threats
- Respond in real time to targeted threats
- Help customers worldwide minimize damage, reduce costs, and ensure business continuity



Securing Your Journey
to the Cloud

ABOUT TREND MICRO[™]

Trend Micro, Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our website at www.trendmicro.com.

TREND MICRO

10101 N. De Anza Blvd.
Cupertino, CA 95014
US toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003
www.trendmicro.com