Tips Provide Guidance for Businesses as They Integrate Social Media Strategies into their Core Businesses

ORLANDO, Fla., /PRNewswire/ -- Panda Security, The Cloud Security Company, is providing guidance to small-to-medium sized businesses (SMBs) on ways to safely and securely integrate social media strategies into their businesses. After conducting its 1st Annual Social Media Risk Index for SMBs last September, Panda Security discovered that 78 percent use social networking sites to support research and competitive intelligence, improve customer service, drive public relations and marketing initiatives and directly generate revenue. However, corporate social media strategies and security policies usually overlook crisis management plans to face the challenges posed by social media, and authenticity, security and privacy continue to be of utmost concern.

Protecting brand or digital identity should be a priority for all businesses, but in reality, neither the top social media platforms nor companies themselves seem to pay much attention to it. The fact that anybody can create a fake online profile in the name of a real business means that people can speak on behalf of a company without having anything to do with it. This could lead to the creation of communities of users tricked into believing that a corporate account is authentic. It could also lead to publication of information that could damage the brand and result in public relations disasters.

Only a few social media sites like Twitter allow users to show their account is authentic through a Verified Badge, but most of them do not include that option. It is therefore recommended to proactively register all company trade names on the main social media sites, clearly identifying a business official communication channel if there is no other verification mechanism available.

Companies are affected by the same problems as individual users are who connect to social media sites. The main security concerns businesses should monitor for include:

* Identity theft: Administrators could become infected and have their profile login data and passwords compromised. This could result in anybody taking control of the corporate account to perform actions including scheduling events (on Facebook, for example) with malware links. Similarly, a malicious user that takes over an account could post information from a company's official profile with disastrous effects.

* Infection risks: Attackers could take advantage of instant messaging applications or the timeline feature in microblogging platforms to send users information with hidden links to malware sites. In the case of large corporations, this could result in targeted attacks designed to infect users' computers in order to penetrate networks and access confidential information. Similarly, malicious links can be posted on

profile walls contributing to the spread of computer malware. Any of these actions could clearly compromise brand integrity.

* Platform vulnerabilities: 2010 saw a number of security exploits in popular social networks like Facebook or Twitter, putting millions of users at risk. As more users join these sites, there will be more researchers looking for security flaws, so users must be aware that the platforms will become more vulnerable as time wears on.

Following good password management practices like changing them regularly and strengthening them through the combination of alphanumeric characters can help protect corporate integrity. Security awareness and education as well as keeping oneself up to date on the latest security threats will help corporate profile administrators to stay alert and detect any irregular activities.

The study showed that 77 percent of SMB employees use social networking during working hours and could share confidential information there. This information can potentially be used by malicious users to post information about corporate finances, practices or internal work processes, which becomes a major risk. Adequate training programs and social media policies will greatly minimize the risk of confidential information leaks.

According to Luis Corrons, Technical Director at PandaLabs, "In the past, most social media sites were for personal use, but now we are witnessing a boom of social media strategies in the corporate sector. Web 2.0. has proven to be an extremely efficient way to implement marketing, communication and customer service activities, but companies must understand the risks involved in these channels."

"Corporate security plans, whether for large or small businesses, must include contingency action plans in the event of public crises caused by any of these online platforms and resulting in reputation damage and financial losses. It is clear that cybercriminals will start shifting their attention to companies using social media as corporations return much more benefits than individual users."

To access the Social Media Risk for SMBs in its entirety, please click the following link: http://prensa.pandasecurity.com/wp-content/uploads/2010/06/1st-Annual-Social-Media-Risk-Index-Slidedeck.pdf