



Social networks favourite targets of cyber criminals: Sophos

Top sites pose risks to firms whose employees have access

By Veronica C. Silva
04 Feb 2010

Manila, 4 February 2010 – Social networking sites are currently the favourite targets of cyber criminals, according to the latest report of IT security firm Sophos.

Sophos' 2009 Security Threat Report 2010, which included a focus on social security, noted an increase in spam and malware attacks in the past 12 months through top social networking sites, such as Facebook and Twitter, as more people join and participate in these social media.

The report noted that 57 per cent of users have been spammed via social networking sites, a rise of 70.6 per cent from last year. Another 36 per cent reveal they have been sent malware via social networking sites, a rise of 69.8 per cent from last year.

Sophos surveyed 500 organisations and 60 per cent of respondents said they believe "Facebook presents the biggest security risk of the social networking sites, significantly ahead of MySpace, Twitter and LinkedIn."

Most respondents, or over 72 per cent, believe their employees' behaviour on these social networking sites could pose a risk to their business security. The number has increased from 66 per cent in a previous study.

The Sophos report quoted a Cisco report which said almost two per cent of all online clicks last year through 4,000 Cisco Web security appliances have been on social networking sites, 1.35 per cent on Facebook alone.

Dramatic rise in attacks

"The dramatic rise in attacks in the last year tells us that social networks and their millions of users have to do more to protect themselves from organised cyber crime, or risk falling prey to identity theft schemes, scams, and malware attacks," said Graham Cluley, senior technology consultant for Sophos.

Sophos said this should be a concern for firms whose employees may be putting the organisation at risk by their participation in social networks. The same survey revealed that 49 per cent of firms allow all their staff "unfettered" access to Facebook, a 13 per cent rise from a year ago.

Facebook is currently one of the top social networking sites with 350 million users as of December 2009.

But Sophos is asking companies to think of more creative ways to prevent Internet attacks from spreading throughout the organisation instead of a blanket ban on the use of social networks at work.

The security company is also quick to defend Facebook, which recently has been implementing many security and privacy settings to the extent that some of its users are already complaining.

Said Cluley: "The truth is that the security team at Facebook works hard to counter threats on their site. It's just that policing 350 million users can't be an easy job for anyone. But there is no doubt that simple changes could make Facebook users safer. For instance, when Facebook rolled out its new recommended privacy settings late last year, it was a backward step, encouraging many users to share their information with everybody on the Internet."

Social security

Cluley noted that social networking is part of today's business and that the solution could be to implement some form of "social security".

Aside from Facebook, the Sophos report noted networking site LinkedIn is likewise a threat to companies even if it is the most "less threatening" among the social networking sites.

Users of LinkedIn, which is more of a business-networking site, reveal some corporate information such as the size of companies and positions in the organisational structure.

Sophos said it would be easy for cyber criminals to victimise social network users by using their e-mail addresses provided in such websites.

Tags: Cyber-crime