



# Security expert alarmed by rising attacks on social networks users

By **NetworkWorld Asia Staff** | Feb 3, 2010

IT security and data protection firm Sophos warns there is an alarming rise in attacks on users of social networks, such as Facebook and Twitter, by cybercriminals.

Sophos's "Social Security" investigation reveals that criminals have increasingly focused attacks on social networking users in the last 12 months, with an explosion in the reports of spam and malware. Fifty-seven percent of users report they have been spammed via social networking sites, a rise of 70.6% from last year. Meanwhile, 36% reveal they have been sent malware via social networking sites, a rise of 69.8% from last year.

"Computer users are spending more time on social networks, sharing sensitive and valuable personal information, and hackers have sniffed out where the money is to be made," said Graham Cluley, senior technology consultant for Sophos. "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 cybercrime, or risk falling prey to identity theft schemes, scams, and malware attacks."

Sophos surveyed over 500 organisations, and discovered that 72% are concerned that employee behaviour on social networking sites exposes their businesses to danger, and puts corporate infrastructure - and the sensitive data stored upon it - at risk.

The "Social Security" survey is just one part of Sophos's 2010 Security Threat Report, which explores current and emerging computer security trends. It reveals that criminals identify potential victims on social networks, and then attack them, both at home and at work. In Sophos's opinion, many Web 2.0 sites are concentrating too much on growing their market share at the expense of properly defending their existing users from internet threats.

## Facebook: Most feared social network

Survey respondents were also asked which social network they believed posed the biggest security risk, with 60% naming Facebook, followed by MySpace (18%), Twitter (17%), LinkedIn (4%).

"We shouldn't forget that Facebook is by far the largest social network - and you'll find more bad apples in the biggest orchard," explained 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 backwards step, encouraging many users to share their information with everybody on the internet."

Sophos's Threat Report also reveals that 49% of firms allow all their staff unfettered access to Facebook, a 13% rise on a year ago.

"The grim irony is that just as companies are loosening their attitude to staff activity on social networks, the threat of malware, spam, phishing and identity theft on Facebook is increasing," said Cluley. "However, social networks can be an essential part of the business mix today, and the answer is not to bar staff from participating in them but to apply some 'social security' instead."

Although LinkedIn is considered to be by far the least threatening of the networks, Sophos advises that it can still provide a sizeable pool of information for hackers.

"Targeted attacks against companies are in the news at the moment, and the more information a criminal can get about your organisation's structure, the easier for them to send a poisoned attachment to precisely the person whose computer they want to break into," explained Cluley. "Sites like LinkedIn provide hackers with what is effectively a corporate directory, listing your staff's names and positions. This makes it child's play to reverse-engineer the email addresses of potential victims."