

IT



RELATED TOPICS

[Facebook](#), [information technology](#), [internet](#), [online security](#), [scam](#), [social media](#), [social networking](#), [Sophos](#), [theft](#)

CATEGORIES

[Technology](#) | [Social media](#) | [Internet](#) | [IT](#)

PEOPLE

[Paul Ducklin](#)

COMPANIES

[Facebook](#), [Sophos](#)

Social media security threats on the rise

By Michelle Hammond
Friday, 21 January 2011

Small businesses are being urged to ramp up their security measures around social media, with a new report revealing a 90% increase since 2009 of social networking users being sent vicious malware.

IT security and control firm Sophos has released its latest Social Security survey as part of its annual Security Threat Report, detailing the IT security threats that social networking users need to watch out for in 2011.

The survey, which charts users' experience of social networking, particularly in the workplace, reveals 67% of respondents have been spammed via social networking sites; more than double the figure reported less than two years ago.

According to the survey, 40% of respondents have been sent malware such as worms while 43% have been the recipients of phishing attacks.

Paul Ducklin, head of technology at Sophos Asia Pacific, says social media represents a new era of IT security threats.

"Rogue applications, click-jacking, survey scams – all unheard of just a couple of years ago – are now popping up on a daily basis on social networks such as Facebook," Paul Ducklin says.

"People need to be very careful they don't end up being conned for their personal details, or get tricked into clicking on links that could earn money for cybercriminals or infect innocent computers."

The Sophos survey reveals 59% of respondents believe employee behaviour on social networking sites can endanger corporate network security, while 57% are concerned their colleagues are sharing too much information on social networks.

However, Ducklin says total bans on employees accessing social networking sites are becoming rarer.

"More firms recognise the value such sites can bring in raising brand awareness and delivering social media marketing campaigns," Ducklin says.

"If your business isn't on Facebook but your competitors are, you are going to be at a disadvantage. But you have to be aware of the risks and secure your users while they're online."

According to Sophos, cybercrime continues to encroaching into the business space, citing industrial espionage, spear phishing and mass theft of customer information as increasingly difficult to detect.

"Increasing amounts of sensitive data is stored, accessed and manipulated in databases connected to company websites as businesses increasingly interact with their customers through the internet," Sophos says.

"At the same time, network boundaries are becoming ever more indistinct and porous as new technologies enable greater access from remote workers and mobile devices," Sophos says.

Sophos says in addition to protecting networking boundaries, businesses and website

maintainers are under growing pressure to ensure their web presence provides adequate protection for the users of its web services, particularly social media sites.

Sophos offers up some tips for business owners and their employees:

1. Remember that if something sounds too good to be true, it probably is.
2. Ask yourself – why would you be singled out for a windfall or other special treatment out of the millions of other internet users? If you can't find a good reason, it's probably a scam.
3. Don't believe everything you read. Just because an email or website is presented attractively doesn't mean it's telling you the truth.
4. Stop to think. Victims of internet crime often act on impulse by clicking on an attractive link or attachment without thinking of the possible consequences.
5. Unless you're certain of a person's identity and authority to request such information, never provide your personal details or company information.
6. Avoid revealing personal or financial information in an email, and be wary of emails that ask you to follow a link to enter such information.
7. If you think an email may not be legitimate, attempt to verify it by contacting the company or organisation directly.
8. Double-check the URLs of websites you visit. Some phishing websites look identical to the actual site but the URL could be subtly different.
9. Be cautious about sending sensitive information over the internet if you're not confident about the security of the website.
10. Be suspicious of unsolicited phone calls and emails that ask for information about your employees or other information.

Like

One person likes this.

0

SHARE THIS PAGE :

RELATED ARTICLES :

[Reset your password on Mac OS X](#)

[THE NEWS WRAP: Report says Australian housing affordability among worst in the world](#)

[Check your WiFi stats in Mac OS X](#)

[Start-ups well placed with staff spending](#)

[Should I enlist the services of a so-called 'social media expert'?](#)