Small Business Security Guides

Social Networking for Business: Risk or ROI?

AVG | AT WORK

Social Networking for Business: Risk or ROI?

LinkedIn, FaceBook, Twitter and social networking in general are argued by some to have tangible business benefits, but are these communication channels nothing more than a corporate risk gateway or do they have the potential to deliver a real and positive impact upon total Return on Investment (ROI)?

Did You Know?

- Leading research and advisory company Gartner predicts social networking to overtake email by 2014 http://www.computerworlduk.com/management/online/new-media/news/index.cfm?newsid=21033

- A Manpower survey in January 2010 indicated that only 20% of companies worldwide have a social media policy. http://www.changeboard.com/resources/article/3404/social-media-the-employment-law-lowdown/

- The Numbers of LinkedIn members grew by 40% in the first six months of 2010 http://econsultancy.com/blog/6205-revised-mind-blowing-social-media-statistics-revisited-and-20+-more

- 40 percent of businesses globally have successfully used social media for business development, according to a new survey by Regus. http://www.regus.presscentre.com/Press-Releases/34-Percent-of-Canadian-Businesses-Have-Used-Social-Media-to-Win-New-Business-38b.aspx

According to FaceBook founder Mark Zuckerberg, "..people are a lot more relaxed about online privacy than they used to be. Attitudes have changed and people have "opened up on the web" as they share information about themselves on social networking sites. .."Although this action in itself is not without its personal privacy risks, the real issue arises when users take this approach with them to work and are equally "open" in a corporate business environment.

The perceived shift in attitudes about personal information sharing among its user-base was behind FaceBook's decision to change its privacy rules late in 2009. But while the changes were deemed to be bold and brave by FaceBook insiders, some of its 350 million worldwide users felt otherwise and so complained that the company was out of step with very real concerns about identity theft and online security.

Industry opinion suggests that there while has been an adoption of FaceBook (and perhaps even more prevalently on LinkedIn and Twitter) as a business-level social networking tool, the privacy augmentations that the social networking giant brought to bear were not commensurate to the risks that now exist at the corporate networked level. Put simply, if we use social networks inside a business network then a new privacy policy alone doesn't cut it. Without directly addressing the issues of identity theft, cybercrime and web-driven targeted espionage attacks then we are leaving the door wide open.

Social networking sites in the meantime appear to be focused on how to make sites more engaging, easier to use and more 'sticky' to hold users' attention. A central part of this is getting users to post more personal content and link in with more personally connected information. All of which builds up profile and identity. Take this example to the business environment and identity becomes intellectual property – and this needs to be locked down.

Once again, take this example into the workplace and you can see where the dangers lurk. Sending out information detailing which companies you are meeting with highlights your business partners and prospects to your competitors. Telling the world about your company's new product innovations prior to their official launch will not earn your colleague's respect for sure. Perhaps worst of all, pump out details of which companies you can't stand dealing with and whose products you hate and you might just be one step away from a defamatory court case.

The danger of an unguarded approach to social networking is not just about risks to physical property on a personal or corporate level; identity theft is also a serious concern. The US government's StaySafeOnline site (http://www.staysafeonline.org/ has some useful advice on how to use social networking sites safely. "Online social networks have sprung up for business, hobbies, schools and religious groups," the site states. "Used properly, they are a unique communications tool to keep in touch with friends and colleagues. But like any online tools, social networking sites can be abused by hackers and cybercriminals."

StaySafeOnline warn that both casual and business users should be careful what they post online as criminals use the sites to trawl for information that they can exploit, so it is an essential process to get acquainted with the privacy settings and tools on the social networks that you use. The bottom line is – all employees should be aware of which social sites a company allows employees to use during working hours.

A new term to learn – gateway data

So how exactly could a cybercriminal use information from a FaceBook or LinkedIn profile to get access to a corporate or personal bank account for instance? Herbert "Hugh" Thompson, professor in the Computer Science department at Columbia University in New York, has coined the term "gateway data" to refer to the confidential information harvested from social networks sites.

Thompson argues that at some point there has got to be some fall-out from the over-sharing of information via social media. "Criminals have got to be able to leverage the information that people are sharing to do harm at some point - and I now think we have gotten to that point," he says.

The gateway data identified by Thompson can be used in a variety of ways. For example, discovering someone's Mother's maiden name from FaceBook could in turn be used to answer a password prompt question on an email account. Even if that account is a personal account, the user will have been compromised and the hacker is one step closer to all the corporate information that they want.

Once a criminal has gained access to the user's email there is good chance there will be details inside of how to break into a bank account for example. Other uses for gateway data include using a partial piece of information, such as the first five digits of a company credit card, to trick the user into revealing the full card number.

Basically a hacker will be looking to use lots of fragments of data to reveal a larger piece of confidential information. So the separation between your personal and business data is not as distinct as you might think, in fact there could no boundaries between them at all.

In addition to following the safe and sensible approaches prescribed by StaySafeOnline, other experts advise against installing applications from social networking sites unless the application itself is from a trusted source – and this in itself is a highly subjective judgement to make, as who do you know who you can really trust and how do you know that they themselves have not already been compromised?

"Develop a healthy dose of scepticism," advises Roger Thompson, chief researcher with Internet security company AVG. "When you get one of those offers to watch a video and you have to install something to watch the video - don't do it. It's not worth it and you should never have to do that.

These unknown applications can often contain malicious code such as viruses or worms and an enticing video is precisely the kind of tool that criminals will try and virally disseminate on the web," added Thompson.

AVG has also warned about the popularity of shortened URLs on sites such as Twitter. “The problem with shortened links is that they usually don’t bear any resemblance to the original URLs, which means that users don’t always know what they’re clicking. People click with the intention of going to a specific site, but the link can be easily hacked to send them to a site containing Trojans, spyware, rootkits and other malware instead,” explains Thompson.

In summary, social networking can represent a positive force within a corporate communications environment and contribute positively to a profitable bottom line and a business's total ROI from its IT infrastructure. It just needs a layer of management, some user policy controls in place and a degree of strategic planning to ensure that user awareness of the 'corporate voice' is upheld.


AVG SMB group at:
linkedin.com/AVG


Become an AVG Fan at:
facebook.com/avgfree


Read our blogs at:
blogs.avg.com


Follow us at:
twitter.com/
officialAVGnews


Become an AVG
affiliate at:
avg.com/affiliate


Watch our Channel at:
youtube.com/officialAVG

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
Czech Republic
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
United Kingdom
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Deutschland
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com

© 2010 AVG Technologies CZ, s.r.o. All Rights Reserved. AVG is a registered trademark of AVG Technologies CZ, s.r.o.
All other trademarks are the property of their respective owners.