Small Business Security Guides

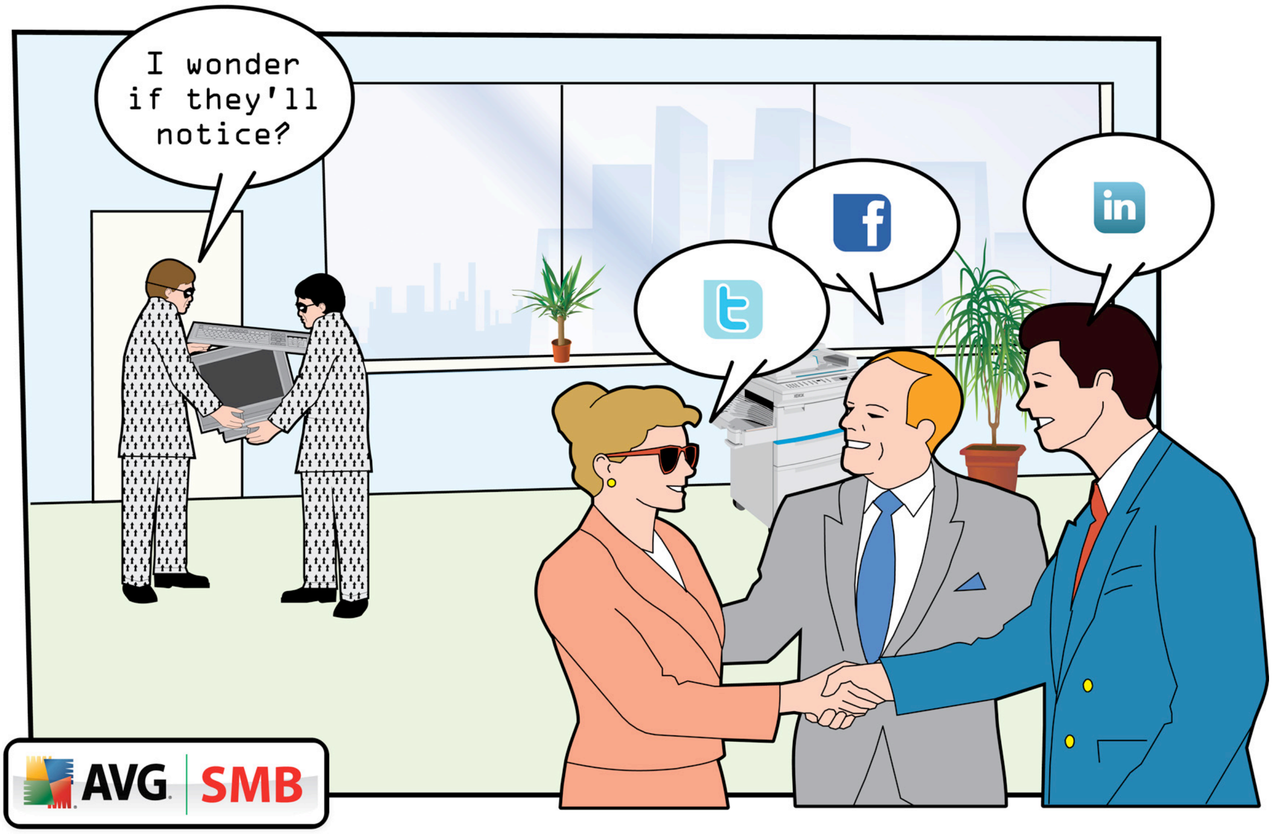
Your Small Business Security Questions Answered: Social Networks, Sensitive Data, Business Banking

AVG | AT WORK

Your Small Business Security Questions Answered: Social Networks, Sensitive Data, Business Banking

Question: If social networks are such a risk, shouldn't we just block them?

When social networking sites such as MySpace and Facebook first emerged, some businesses viewed them as a distraction from work and banned them. With the appearance of other social formats, such as Twitter however, companies have begun to embrace this potential for collaboration. Social networking has evolved from personal networking to become a media for mass communication. Many companies now view sites such as Twitter as a valuable marketing channel.



Given these new legitimate business uses, a policy banning these sites completely seems counterproductive. While serious business roles exist for these tools, for security reasons, companies should still monitor how employees interact with them. Security experts such as Herbert Thompson, a professor in the Computer Science department at Columbia University, has warned about the dangers of revealing personal information on social networks. People may post personal details, for example their Mother's maiden name, that are often used by secure sites as password prompts.

"People are posting indiscriminately – they throw weird information out there. What has happened is there has been a growth in the technology for information sharing but not a commensurate education in what information we should share," he said.

So, while a strict ban of social networking sites may not be the answer, companies should consider creating and enforcing regulations on how they should be used, especially in relation to company business. A recent study conducted by IESE Business School in Spain, E. Philip Saunders, College of Business at the Rochester Institute of Technology in the US, and Henley Business School in the UK, revealed that six out of seven companies don't have a formal policy on how social networks should be used within their businesses. "Ignoring the increased usage and influence of social networking and Web 2.0 tools leaves organizations at the risk of misuse, potentially leading to the disclosure of sensitive information or misrepresentation of the company," said Evgeny Kaganer, Ph.D., lead researcher and assistant professor, IESE Business School.

According to Roger Thompson, AVG's chief research officer, in addition to developing high-level policies for the use of social networks, there are some simple guidelines that managers can provide to staff to minimize the risks.

"The fact that they are so user friendly makes them dangerous. You don't mind your friends knowing where you live, or when your birthday is, or what your mother's maiden name is, but if the bad guys manage to hack into your friend's account, then they find out that information as well," said Thompson.

Thompson advises that something as simple as creating separate passwords for each site, that are also different from log-ins for company systems, can be effective. "If you want to keep yourself safe on these sites then you should use a unique user ID and password for each one or at least a unique password," he says.
Being generally cautious about who staff interact with and what applications they install is a good guideline. "Your mother advised you to never talk to strangers. The same goes for social networking sites, if you don't know who they are, don't talk to them," he added. "Finally, be careful what applications you agree to install. There are a million people developing applications for these sites and something tells me they are not all good guys."

For more on securing social networks see (The Do's and Don'ts on Social Networking, Roger Thompson) (http://www.youtube.com/watch?v=poHqIXvxmfg)

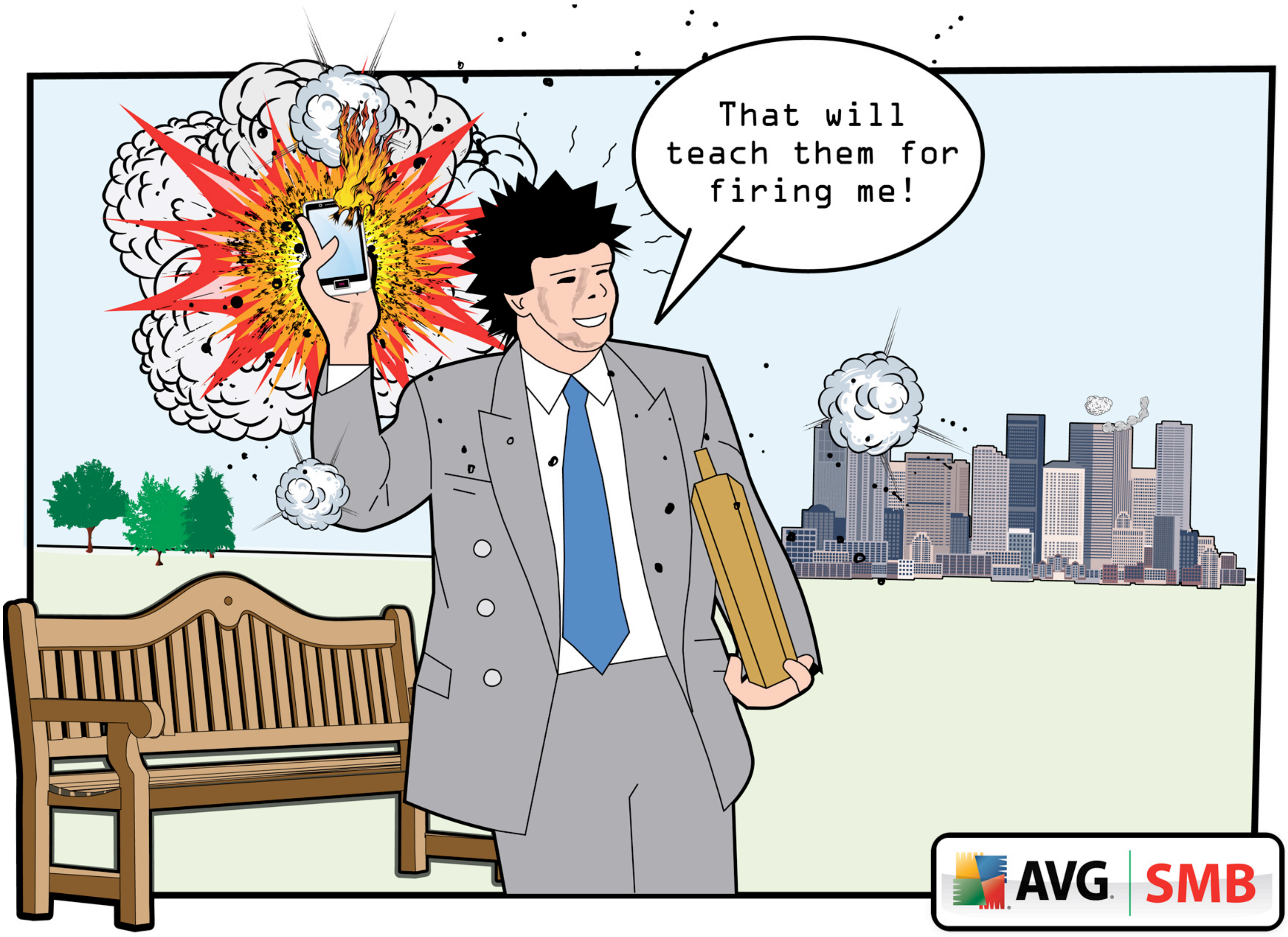
Question: How liable am I for the loss of sensitive data?

The answer to the question of what legal measures companies might face from suffering a data breach or data loss incident depends on a range of factors including the nature of the data in question and where the incident occurred. Obviously, any loss of data could have an impact in terms of negative publicity if disclosed externally, but when it comes to specific legal action, the most stringent rules apply to the loss of data derived from a third-party.

In the US for example, California became the first state in 2003 to pass a law requiring companies to notify customers in the event of a data loss incident, and 44 other states have developed similar legislation in the meantime. A Federal law, H.R. 2221, the Data Accountability and Trust Act (DATA), is also underway but has yet to be passed. DATA would compel companies, no matter what state they happened to be trading in, to reveal to anyone "who is a citizen or resident of the United States whose personal information was acquired by an unauthorized person as a result of such a breach of security" and for the company in question to also notify the the Federal Trade Commission. Although it is not clear what form the legislation will ultimately take, companies that opt to encrypt their data will be looked on more favourably and won't be required to notify everyone concerned if it can be proved that the data is protected or unreadable.

The UK is also planning to tighten up its rules on protecting sensitive data. The Office of the Information Commissioner is tasked with data protection in the UK and has seen its powers gradually increase following a series of government security breaches. Since April 2010, the organization has had the ability to fine companies up to £500,000 if they fail to protect customer data adequately.

Data loss is also an issue for small businesses which often don't have the resources to devote to IT security. According to a 2009 survey from the US National Cyber Security Alliance, 86 percent of the small companies questioned did not have anyone solely concerned with managing IT security and only 28 percent admitted to having any kind of formal IT security policies. The survey also revealed that 66 percent of companies allow the off-site use of PDA's and computers containing sensitive information. (http://www.staysafeonline.org/content/2009-smb-security-studyhttp://www.staysafeonline.org/content/2009-smb-security-study)



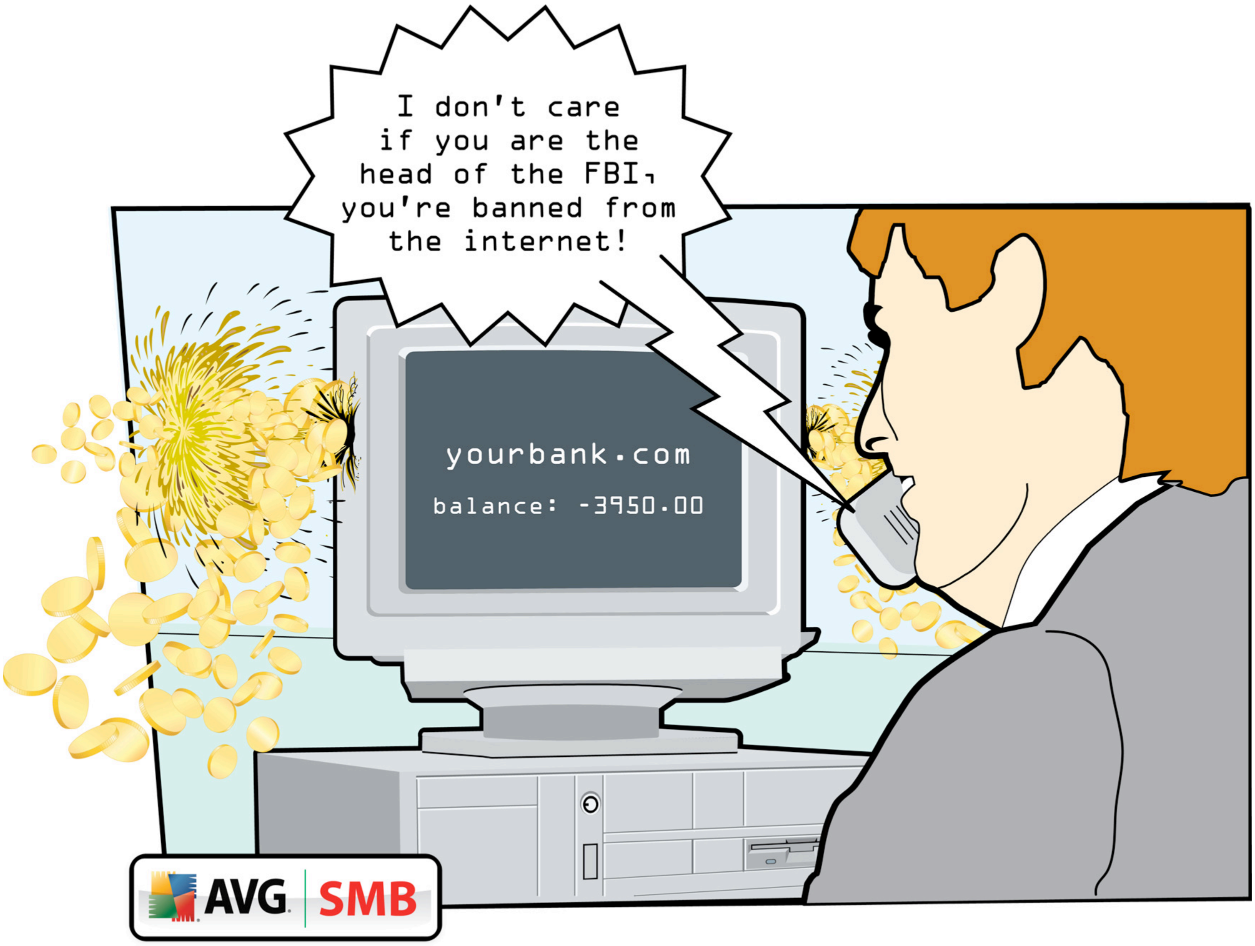
Question: How safe is online business banking?

While businesses and consumers alike are attracted by the flexibility of online banking, it should be noted that this great tool carries inherent security risks. Consider that FBI Director, Robert Mueller, recently announced that he had been banned by his wife from using his service after he nearly became the victim of a phishing scam.

Muller's wife was probably right to be concerned. Figures for the UK alone in 2008 revealed that online fraud had increased by132 percent from 2007. According to UK banking group APACS, Internet only fraud totaled around £52.5m.

For businesses, the threats posed by online banking may be more acute given the dangers associated with so-called "insider threats". IT security experts have long contended that a company's own staff pose a bigger criminal threat than external criminals. While this may no longer be accurate given the the entry of organised criminal gangs in the mid-nineties and the resulting increasing sophistication of cyber-criminals, online banking certainly provides a new channel for these internal or external criminals to steal money or confidential information.

Recent research in the UK from AVG, revealed that the number of financial transactions conducted over the Internet are on the rise, with 85 percent of people now using the Internet for shopping, and over two thirds doing their banking online. The research also showed that fears about cyber theft are rising too, with 43 percent of those surveyed saying they felt more susceptible to cyber theft than burglary, assault, or robbery.


I don't care if you are the head of the FBI, you're banned from the internet!
yourbank.com
balance: -3950.00
AVG SMB

Despite these concerns, the AVG survey also revealed that approximately 30 percent of respondents did not feel they were taking adequate steps to protect themselves. Banks could also be doing more. For example, the use of drop down menus as part of the log-in process can help defeat key-logging software. Criminals use this software to record key-strokes. Drop-down menus can not be recorded in this way as they are activated by the user's mouse. Other approaches include external devices sent to customers which generate unique pin-numbers each time the user accesses their account.
There is general awareness of at least some of the risks associated with online banking, and knowledge of some of the tools that can be employed to combat it. The awareness and knowledge must grow on both sides and, most importantly, once gained should not be ignored.

For more on how to secure online transactions see **How can I protect myself against Cyber Theft? (**http://www.avg.com/77954).

Read more AVG Blogs | Small Business http://small-business.blog.avg.com/2010/02/your-small-business-security-questions-answered-social-networks-sensitive-data-business-banking.html#ixzz0lBnmXlHX
Free Antivirus

AVG SMB group at:
http://bit.ly/avglinkedin

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

AVG | AT WORK