

*GFI White Paper*

# *Social networking malware: The dangers facing SMBs*

Social networking has changed the way businesses communicate with their customers and partners, with most organizations now incorporating social media into their marketing and communications strategies. Unsurprisingly, the popularity of this new media has also created an influx of social-specific malware.

## Contents

Introduction.....	3
Making friends, followers and circles .....	3
The growth of social malware .....	3
The risk to your business.....	3
The need for layered security.....	3
Conclusion.....	4
About GFI VIPRE® Antivirus Business.....	4
About GFI.....	4

This white paper describes the rise of social networking, the types of malware targeting social platforms and how small and medium-sized businesses (SMBs) can protect themselves against the latest social threats.

### *Making friends, followers and circles*

In the first eight months of 2011, Facebook added over 250 million users. Similarly, Tumblr use grew 166 percent this year, with the popular micro-blogging site now boasting 10.7 million users. Today, the average person spends 16 percent of his or her time online at social sites, like Facebook and Tumblr, often checking these sites from work or on company-supplied laptops and smartphones.<sup>1</sup> And employers, for the most part, don't discourage social networking on these devices during off-hours.

### *The growth of social malware*

Recent reports from various security research labs show a 20 to 40 percent increase in malware targeting social networking sites. And cybercriminals are very clever in luring social-site users to unwittingly download viruses and malware. For example, a malicious link may prompt an application or file download to view a news article or video. If a user complies, malware installs on his or her device and quickly spreads throughout their corporate network.

Cybercriminals also benefit from the weak passwords individuals use to log into social sites. They know "many people still use the same username and password for all their online activities, including banking, shopping and email," says Chris Boyd, GFI Software senior threat researcher, and they take advantage of it.

Some malware attacks create a dangerous domino effect, such as hacked Twitter accounts tweeting malicious links to unsuspecting followers and spreading malware exponentially. This chain-reaction malware is not limited to Twitter, as GFI Software found in recent Facebook survey scams. Here, cybercriminals offer free merchandise for participation in surveys and suggest sharing the survey on your Facebook wall, so your friends can also win. At best, those that completed the survey saw an increase in spam. At worst, their personal and financial information was stolen by identity thieves.

### *The risk to your business*

Malicious attacks, on social networks and through other mediums, are the number one cause of data breaches<sup>2</sup>, surpassing lost or stolen laptops and accidental sharing. These attacks impact businesses most notably from a cost perspective. Direct costs include detection, remediation and notification efforts as well as tech support, credit monitoring and legal fees. Based on a review of 51 businesses that suffered data breaches of between 4,200 and 105,000 records, the Ponemon Institute reported the average cost per contaminated record due to a malicious attack as \$318.<sup>3</sup>

Indirect costs of malicious attacks were also considered in the Ponemon Institute estimate. These include IT resources diverted from other projects to focus on repair and damage control as well as sales, marketing, customer service and management teams shifting tasks to emergency communication efforts to repair customer trust.

In addition to increased costs, businesses risk the loss of intellectual property from a malware attack. If a cybercriminal gains access to a corporate network, that company stands to lose new product development plans, confidential marketing or shareholder information and other types of intellectual capital.

<sup>1</sup>comScore, June 2011, [http://blog.comscore.com/2011/06/facebook\\_linkedin\\_twitter\\_tumblr.html](http://blog.comscore.com/2011/06/facebook_linkedin_twitter_tumblr.html)

<sup>2</sup>Ponemon Institute, 2010 Annual Study: U.S. Cost of a Data Breach

<sup>3</sup>Ponemon Institute, 2010 Annual Study: U.S. Cost of a Data Breach

## The need for layered security

Malware attacks are expensive for any company, but for SMBs, costs are magnified. The best strategy for these businesses to protect against social networking malware is a two-pronged approach: education and technology.

The easiest way to prepare employees for the types of malware they may come across is by showing them examples. Share screenshots of Facebook scams, Twitter hacks or fake LinkedIn invitations. Start a monthly newsletter that offers quick tips on avoiding social malware, such as creating strong passwords, only using trustworthy news sources and not clicking on questionable links. When employees realize how convincing these attacks can be, they will also understand how to avoid them.

In addition to employee education, a business antivirus solution is essential in protecting against social malware. Not all AV solutions are equal, and the one you choose should include:

- » **Powerful scanning technology.** High-quality AV solutions will analyze and detect potential viruses and malware before they infect user machines
- » **Active monitoring and protection.** Most SMBs don't have the time or resources to constantly monitor their networks for security threats. Invest in a solution that protects your network and user machines in real time, automatically.
- » **Malicious web filtering.** Block bad URLs before they hit your network with a solution that uses the latest behavioral analysis and malware URL detection technology.

## Conclusion

Rather than face the risks associated with social networking, some SMBs have chosen to ban the use of these applications at the workplace. But in today's interconnected world, where there are real business benefits from social media, this is not a realistic strategy. Companies must take a practical approach in protecting their organizations against malware attacks, by combining employee education with powerful AV security solutions.

## About GFI VIPRE® Antivirus Business

VIPRE Antivirus Business combines the latest antivirus and anti-spyware detection and removal technologies to protect against next-generation malware threats in a comprehensive and highly efficient manner. Built by IT administrators for IT administrators, VIPRE is easy to install, easy to deploy and easy to manage with minimal network and system performance impact. The solution delivers superior endpoint protection against viruses, worms, spyware, Trojans, bots and rootkits via a single, powerful anti-malware engine and wide range of detection methods, including Cobra™ heuristics for first-level heuristic analysis and Active Protection™ for real-time malware detection inside the Windows kernel.

For more information, visit <http://www.gfi.com/business-antivirus-software>.

## About GFI

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMBs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at <http://www.gfi.com>.

## USA, CANADA AND CENTRAL AND SOUTH AMERICA

33 North Garden Ave, Suite 1200, Clearwater, FL USA

Telephone: +1 (888) 688-8457

Fax: +1 (727) 562-5199

[ussales@gfi.com](mailto:ussales@gfi.com)

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

[ussales@gfi.com](mailto:ussales@gfi.com)

## UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

[sales@gfi.co.uk](mailto:sales@gfi.co.uk)

## EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

[sales@gfi.com](mailto:sales@gfi.com)

## AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

[sales@gfiap.com](mailto:sales@gfiap.com)

For a full list of GFI offices/contact details worldwide, please visit <http://www.gfi.com/contactus>



### Disclaimer

© 2011. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.