

Facing Up to the Facebook Dilemma

Networking or Not Working

Who should read this paper

Networking or Not Working

Facing Up to the Facebook Dilemma

Content

Introduction	1
Upsides...and Downsides	1
Cyber-crime and Facebook	1
Facebook Threats: Examples	2
What Policy? Can It Work?	3

Introduction

Connect. Share. Work?

Facebook isn't just a social networking tool. It's a social phenomenon which poses a real dilemma for businesses. Allow employees access...and risk opening a potential Pandora's box of problems? Go for a blanket ban...and lose a valuable channel of communication and collaboration? Opt for a compromise, with use permitted but limited in some way?

This White Paper weighs up Facebook's pros and cons, and shows how to keep your company safe – whatever policy you choose to implement.

Upsides...and Downsides

It's taken the country by storm. Over 9.5 million people in Australia now use Facebook¹. The main purpose may be social, but Facebook also offers real opportunities for businesses. Developing contacts, pooling knowledge, sharing ideas, recruiting top-quality staff, building relationships with customers and partners – it can make key business processes easier, less expensive and more effective, and boost motivation, job satisfaction and team spirit across your workforce.

But for every plus, there's a minus. Facebook can be addictive, leaving some companies to rue giving their employees access during work hours – and to count the cost in dented productivity. This problem is so common that 'social networking' has started to appear in dictionaries.

The medium's 'relaxed' nature can also lure employees into serious lapses of judgement – especially when using corporate hardware out of hours, from home or in another situation where, psychologically, the usual workplace constraints don't seem to apply. It's easy to let slip a confidential nugget of information – or make an off-the-cuff comment, about a customer or competitor, which has explosive consequences. With legal liability resting with the employer, the touchpaper to a time-consuming, financially damaging chain of events may have been lit.

And the dangers don't end there.

Cyber-crime and Facebook

Where internet users go, cyber-criminals follow. Knowing Facebook's sheer size makes it virtually impossible to police. They've devised a bewildering battery of devious techniques to trick and trap users². Hijacking accounts, spreading rogue applications, setting up fake, 'ghost' accounts, posing as Facebook itself – many strategies can be deployed to plant malware on victims' PCs (e.g. via infected weblinks) or harvest personal information (e.g. via 'phish' emails).

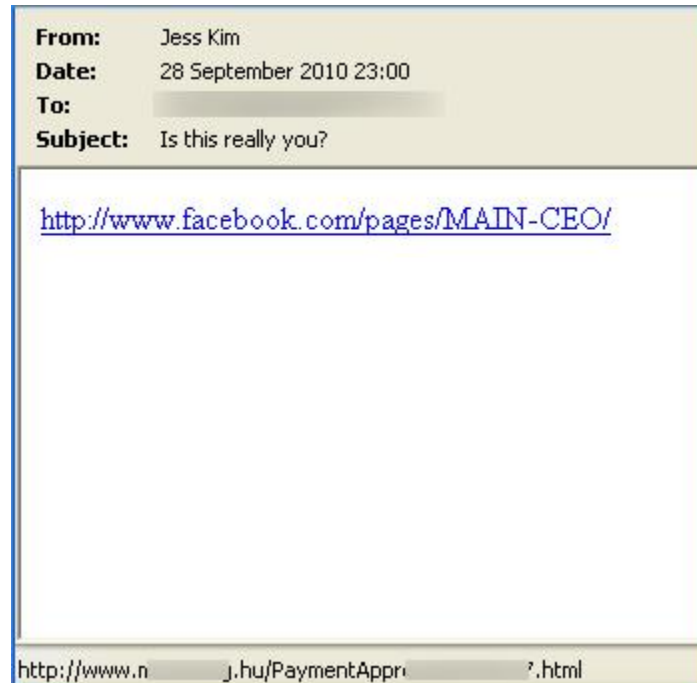
Malware today has real business-bruising potential. Viruses that freeze networks or recruit PCs to botnets; spyware that snoops on browsing behaviour; trojans that secretly burrow in search of sensitive information that can be turned to profit – almost all malware can propagate via Facebook. Some has even been specifically developed to exploit it. For instance, the Koobface worm spreads by sending messages to friends of Facebook users whose machines have already been infected.

But with social engineering now part and parcel of cyber-crime, the loss of personal information via Facebook can be every bit as damaging for a business. Users' names, ages and job titles, for example, can be harnessed to help craft plausible, sniper-like attacks targeting a specific

1-Nick Burcher, Facebook Usage Statistics December 31st 2010 vs Dec 31st 2009 vs Dec 31st 2008, <http://www.nickburcher.com/2011/01/facebook-usage-statistics-dec-31st-2010.html>
2-Facebook (C) 2011, Facebook Security, http://www.facebook.com/security?v=app_4949752878

company or individual – with an email pretending to come from a familiar contact actually containing a malware-infected attachment or linking to an infected website.

As well as using Facebook itself as the vector of attack, cyber-criminals also misappropriate the Facebook name to maximise their chances of a 'hit'. Spam, 'phish' and malicious emails (as well as URLs) may reference Facebook in subject lines, body text, attachment names, web links etc in a bid to slip through spam filters, outwit other defences and coax recipients into complacency:



The Cutwail botnet has made particularly heavy use of Facebook-themed emails to disseminate attachments which, if opened, download the potent 'bredolab' trojan.

Nor are threats, overall, small in number. Symantec.cloud detects countless examples. Facebook-related threats contribute:

- 2% of spam, equivalent to 2-3 billion emails being sent worldwide every day.
- 1.4% of malware, again indicating a massive global problem.

Facebook Threats: Examples

The possible scenarios are endless. But the following examples give a flavour of the problems your business could experience:

1. A cyber-criminal sets up a 'ghost' account, becomes a 'friend' of one of your employees and posts a weblink on their wall. The employee clicks on the link and a data-stealing trojan downloads onto their PC.
2. An employee inadvertently installs a rogue application, which harvests their friends' Facebook data and sends them all a message with a weblink. One of these friends – another employee – clicks on the link, a virus downloads and their PC joins a botnet.
3. An email apparently from Facebook asks one of your employees to update their password and login details. But the email was 'phish' sent by cyber-criminals who use the details to send out spam and to gather information about the victim and their friends – information used to launch a targeted trojan attack on your business.

4. An employee receives an email apparently containing a harmless-looking Facebook weblink. Accessing Facebook from work, they click on the link but it takes them to a pornographic site. The employee makes a claim against your business on the grounds that they weren't adequately protected from such material.

What Policy? Can It Work?

Your Facebook policy needs to reflect the nature of your business, weighing up pros and cons in the context of your business culture, objectives etc. But broadly speaking there are three options, each with its own challenges:

1. Unlimited access – but users need to be safeguarded from rogue applications, camouflaged malware, links to pornographic websites etc.
2. Restricted use – limit access to certain hours and/or user groups via configurable web filtering capabilities
3. Outright ban – this must be implemented using web filtering technology agile enough to prevent employees accessing Facebook both in the workplace and via the corporate network from home etc.

Whatever your decision, how can you ensure your policy is enforced effectively? Awareness-raising education and training will be essential to highlight the policy, explain it and, unless there is an outright ban, promote appropriate, circumspect use of Facebook. But on its own, it simply won't be enough.

Provided by Symantec.cloud, Symantec MessageLabs Web Security Service.cloud delivers a comprehensive, flexible, hosted solution for enforcing any kind of Facebook policy. With industry-leading accuracy in URL blocking/filtering and malware/infected link detection, its ability to stay relentlessly ahead of existing and new threats is rooted in three key differentiators:

1. The unique global infrastructure underpinning Symantec.cloud services.
2. The unmatched threat detection capabilities of Skeptic™ – proprietary Symantec.cloud technology.
3. The unsurpassed customer service and support levels delivered by Symantec.cloud.

Wherever a threat lurks, the service spots it and blocks any request to open the page or file, follow the link, access the application etc. What's more, the service is completely customisable, so you can set up and monitor different rules for different user groups – even for individual employees. Employees can also have different levels of Facebook access at different times of the day.

Coupled with Email Security Service.cloud, which provides comprehensive protection from spam and malicious emails, Web Security Service.cloud really can make your policy work – and help you solve the Facebook dilemma.

About Symantec.cloud

Symantec.cloud, a division of Symantec Corporation, offers customers the ability to work more productively in a connected world. More than 31,000 organizations ranging from small businesses to the Fortune 500 across 100 countries use Symantec.cloud to administer, monitor, and protect their information resources more effectively. Organizations can choose from 14 pre-integrated applications to help secure and manage their business even as new technologies and devices are introduced and traditional boundaries of the workplace disappear. Services are delivered on a highly scalable, reliable and energy-efficient global infrastructure built on fourteen datacenters around the globe.

Symantec.cloud
Symantec Corp.
Level 14, 207 Kent Street,
Sydney NSW 2000 AUSTRALIA
Tel: +61 2 8220 7000
Fax: +61 2 8220 7075

Symantec helps organizations secure and manage their information-driven world with managed services, exchange spam filter, managed security services, and email antivirus.

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
11/2011