AdviSec Ltd

Whitepaper

Social networking and the security issues

March 2011

1 Introduction

1.1 Aim

This paper provides an overview of 'social networking' applications, including the potential business benefits (see examples below). The paper also highlights security issues that management need to be aware of when business afford their staff access to social network sites, and which if not addressed are likely to result in the compromise of business data, IT resource or staff. Finally the paper provides recommendations for addressing the security issues.

"Avon and Somerset police have launched a Facebook viral campaign in a bid to reduce the number of incidents of rape and sexual assault amongst young people during the summer holidays."

"Avon and Somerset Police have placed an advert on the social networking site which encourages people to contact their incident room with information about the murder of Joanna Yeates"

"Networking Women in the Fire Service (NWFS) is a network of and for all fire service women, whether operational or not. It has grown to become an independent national organisation providing networking, support and education for all women who work in the British Fire Service. It is also a source of information for employers and others concerned with making the Fire Service a place where women and men can work together harmoniously and professionally."

1.2 Background

Social networking refers to an online service, platform, or site that focuses on building and reflecting relationships between people who usually share interests and/or activities[1]. A social network service consists of a representation of each user (often referred to as a profile), his/her social links, and a variety of additional services. This service allows users to share ideas, activities, events, and interests within their individual networks.

Social networking, whether it be Facebook, MySpace, LinkedIn, YouTube or Twitter, is fast becoming a way of life for millions of people for personal or business reasons, but it comes with risks that include identity theft, malware infections and the potential for reckless remarks that damage corporate and personal reputations. For example, for the period 2009, 57% of users claim

[1] e.g. friendship, kinship, common interest, financial exchange, dislike, sexual relationships, or relationships of beliefs, knowledge or prestige

they were spammed via social networking sites and 36% of users claim they were sent malware via social networking sites[2]. Examples of 'scams' are described below.

Sophos has surveyed more than 500 organizations, discovering that 72% of them think social networks are a danger to their company.

Finally social networking is predominantly based on public-facing sites[3] at present, however there is some interest in the deployment of such technologies within corporate networks, which may be due in part to the perceived security risks.

1.3 Examples[4]

1.3.1 The Nigerian 419

The Scam: It may sound like a hip new emo band (or a somewhat old e-mail scam), but the Nigerian 419 will do more than just offend your ears--it'll also empty your wallet. The moniker refers to a scam dating back decades that has recently entered the social network scene.

Back to Beny Rubinstein. A couple of months ago, Rubinstein received some alarming Facebook messages from a friend and fellow tech professional.

"[He said] he was in the UK and was robbed, and needed $600 to fly back to Seattle," Rubinstein recalls.

The messages came both in Facebook-based IMs and in e-mail. They included details such as family members' names, making the notes appear all the more authentic. It wasn't until 2 hours and $1100 later that Rubinstein realized what had happened: Someone had hijacked his buddy's account, contacted his friends, and--at their expense--made off like a bandit.

"Scammers figured out that even though social networks don't have direct access to money, they have access to information that gives you a good shot at getting someone else's money," says Vicente Silveira, a product management director at VeriSign and a personal friend of Rubinstein's.

The Protection: Before you send cash to a pal who seems to be in trouble, try to contact him or her outside of the social network--either by phone or by external e-mail. Not feasible? Ask an extremely personal question that a hacker couldn't possibly figure out from information within the profile. We'll leave the specifics up to you.

---

[2] Sophos

[3] Accessible via the Internet

[4] Taken from "JR Raphael, PC World"

1.3.2 The Widget Warrior

The Scam: Facebook is famous for its widgets--you know, the third-party applications that you can add onto your account. Sometimes, though, widgets turn into warriors with a single mission: stealing your data.

The first rogue widget reared its head in 2008, when researchers realized that a program called Secret Crush had anything but sweet intentions. The application, which was supposed to help you find your virtual admirers, instead installed spyware onto your computer. Even worse, it encouraged you to spread the love by getting other friends on-board--essentially "manipulating humans to pass it along on their own," says Guillaume Lovet, senior manager of Fortinet's Threat Response Team.

Secret Crush has since been crippled, but the potential for similar threats still exists. Just days ago, security experts determined that an application called Error Check System was misusing profile details and possibly stealing personal information. A few months earlier, researchers from Greece's Institute of Computer Science uploaded a malicious app to Facebook as an experiment (PDF). The team was able to configure the widget, which posed as a "Photo of the Day" displayer, to utilize its users' Internet connections for denial-of-service attacks.

The Protection: Use extra caution when installing third-party applications. "When you accept to install one, malicious or not, you are granting its author access to all the info in your profile," Lovet says. Make sure you know what the app's creator will do with it.

1.3.3 The Koobface Virus

The Scam: Don't be fooled by the name--there's little to laugh about when it comes to the quickly spreading Koobface virus. (The word, by the way, is an anagram of "Facebook.") Once the virus infects your PC, it starts sending messages or wall postings to your Facebook friends, directing them to a "hilarious video" or some "scandalous photos" of someone you both know.

"The link promises an enticing video, but when the user clicks, he is presented with a Web page with a fake Adobe Flash update or a fake codec that needs to be downloaded," explains Ryan Naraine, a security evangelist with Kaspersky Lab. "That download is malware."

The Protection: Antivirus software can help keep you safe, but some common sense can also go a long way. "Be wary of any kind of direct URL in messages or postings," advises Jamz Yaneza, a threat research manager with Trend Micro. If a site asks you to download a software update, Yaneza says, click Cancel and go directly to the vendor's page to see if the update is legit.

1.3.4 The Phishing Pond

The Scam: Phishing, a favorite hacker tactic, has found new life at social networking sites. Scammers trick users into following links that open official-looking Facebook log-in prompts. If you enter your user name and password, the information is logged--and your account is theirs.

Brandon Donaldson, a pastor at the Lifechurch.tv Internet Campus, fell for the scam. Someone gained control of his Facebook account and started sending messages to his friends and followers, trying to persuade them to follow the same links and unwittingly give up their accounts, too.

"This was a pretty bad ordeal, since I regularly put video content up on the Web, and I use the Internet as a tool for many relationships," Donaldson says. "You build a certain social trust in these spaces, and you want to keep that trust without these kinds of incidents."

The Protection: The previous plan also applies here: Watch where you click. Plus, if you're ever asked for your password midsession, don't enter it. Manually navigate back to the Facebook.com home page instead, and then log in there if need be.

1.3.5 The Contrived Community

The Scam: Community enthusiasts, be cautioned: Facebook user groups can sometimes be cleverly disguised vehicles for marketing. And--whether you realize it or not--when you click the join link, you're effectively opting in.

Brad J. Ward was one of the first users to find such a scheme in action. Ward, then a member of Butler University's admissions department, discovered a Facebook group called "Butler Class of 2013." The only problem: The people behind it had nothing to do with Butler. After posting about the issue on his blog SquaredPeg.com, Ward soon learned that the names of nearly 400 other schools appeared in similarly suspicious groups, all created by the same small set of people.

"My initial reaction was that some company or person was essentially setting themselves up to be the administrator for hundreds of groups, which provides the opportunity to send out mass messages or to collect data," Ward says.

His instinct was right: The publisher of a college guidebook had set up the groups, seemingly with the goal of building a mass mailing list for marketing its products, Ward discovered.

"Was any of it illegal? Not necessarily," Ward points out. "But was it unethical, and could it be misconstrued as an official university presence? Yes."

Once exposed, the publishing company College Prowler admitted its involvement and agreed to back out of the groups. Still, that's only one company. More than likely, countless others haven't been detected, and are actively using groups to gain the trust (and information) of unsuspecting users.

The Protection: Be very selective in deciding what groups you join. If you aren't sure who runs a given Facebook community, or whether it's officially linked to the organization that it claims to be, don't accept the request. Your privacy is worth more than any membership.

In the end, staying safe comes down to maintaining control of your information and carefully selecting with whom you share it--because you never truly know who's on the other end of electronic communication. This past month, for example, a high school student was charged with 12 felonies after investigators say he posed as a girl on Facebook and tricked male classmates into sending him nude photos.

2 Responsibilities

This section highlights a number of key points regarding the responsibilities of individuals and their respective employer that must be respected when social networking:

1. Legal: Organisations are responsible for the actions of their employees when organisational assets are used implement the actions[5]. Note this includes provision made by organisations for ‘personal matters’.
2. Actions by individuals ‘outside of the work place’ must respect the roles which they undertake in society. Furthermore there are several examples where organisations have lost staff due to carelessness in using social networking sites on a ‘private-basis’.

This whitepaper is aimed at ensuring that the points raised above are addressed.

[5] Including laws, regulations and Codes of Practice

3 Social networking sites

3.1 How are Social networks used?

1. Access to social networks may be undertaken from a wide variety of devices, including desktop computers, laptops, tablet devices and Smart phones[67]. It is also worth noting that:
    - Many Smart phones belong to individuals rather than the organisation
    - Smart phones facilitate access to a small number of corporate applications, e.g. email, calendar and contacts
2. In general users do not pay sufficient attention to the configuration of their accounts, including in particular setting access rights with regard to their information assets. Annex A provides further details of 'privacy settings' in Facebook, for example.

   Minimum password standards vary in 'quality' terms between social networking sites. For example, Facebook requires only a six character password with complexity.
3. Users do not always pay sufficient attention to what they post. Furthermore users need to be aware that posted information stays around for many years and could come back to haunt them.
4. Access to social networking sites is undertaken using HTTP, and unless web-content filtering software is employed, will pass straight-through an organisations' Internet firewall.

   Access to social networking sites is via a browser or dedicated client software.

   Twitter was different from other social networking sites in that users provided content by 'tweeting' using SMS from mobile phones. However other social networking sites are starting to provide this same capability.

[6] It is asserted that these devices are equipped with WiFi and GPRS / 3G capabilities.

[7] Whether we like it or not, a wide range of SmartPhones are on the market, i.e. Blackberry, Windows mobile devices, Android-based devices and IPhones. Note the preference would always be to use an assured device (e.g. UK CAPS scheme, FIPS 140-2)

5. University of Virginia researchers have discovered that 90.7 percent of Facebook's most popular applications have access to users' private data, whether they need it or not, leaving users exposed to targeted phishing attacks and identity theft. Moreover Facebook permits application developers to get access to large amounts of sensitive data, all without clear user consent. Simply put, whenever a user installs a Facebook app, the developers of that application get access to data on every person who that user is Facebook 'friends' with, as well as most of the people in that user's network. While Facebook makes it perfectly clear when users install an application that developers will get access to their data, it doesn't do anything at all to warn users that the same data sharing occurs when their friends install apps.
6. Corporate policy statements in respect of social networking are rare.
7. Not many users read the terms and conditions of use.

3.2 Business benefits of social networks?

The following list represents the potential 'benefits' to business of engaging with social networking sites.

- Tracking down individuals, based on various search criteria, e.g. identity, industry accreditations, social and/or work interests.
- Maintaining contact with individuals, together with their current situation and views on subject matters.
- Reference material with regard to individuals[8].
- Sharing information on particular subject matters with individuals based on 'communities of interest'
- Opportunity to seek opinions on specific subject matters

[8] Implications with regard to employment law

4 Security risks

4.1 Social networking site?

What assurance do we have that a social networking site is secure? If it isn't, then asking users to configure account settings and adopt 'good practice' is pointless. Answering the question requires that we consider:

- Platform security
- Core social network application[9]
- Third party applications / widgets[10]. For example with regard to Facebook, developers must have access to a Web server where applications are stored, i.e. Facebook does not host third-party programs; furthermore applications can be Web-based, desktop-based or mobile-device-based.

4.2 End-user devices

- Whilst some risks are common across all categories of device (e.g. reckless remarks and Identity theft) other risks vary significantly depending on the operating system (e.g. threat from malicious code).

4.3 Too much Trust?

- Social networking sites are good for pulling together groups of people with similar backgrounds or interests. How that information gets used depends on the intentions of those using it.
- It's simple for a 'hacker' to set up a phony ID on a social networking site and gain the trust of people. Thereafter it is straightforward to lead 'friends' to a phishing site, where account details for more 'lucrative' systems can be obtained.
- Platform and Social network applications (including third party sites) are not 'accredited' with regard to minimum security standards. Hence the 'trust' (or confidence) that users can have in Social networks has to be questioned.
- Developer issues, for example Facebook's terms of service say developers can't abuse the Facebook data they access, there's no way for Facebook to enforce that.

[9] As well as Facebook, other major social networks like Twitter have been found to contain major loopholes that can be exploited by hackers to gain access to passwords and other private information.

[10] Widgets may be looked upon as downloadable applications which look and act like traditional apps but are implemented using web technologies including JavaScript, Flash, HTML and CSS. Widgets use and depend on web APIs exposed either by the browser or by a widget engine

5 Recommendations

5.1 Policy

Create a corporate policy for social networking.

Implement awareness of the corporate policy through training exercises, e.g. multiple choice exam.

Monitor compliance with regard to the corporate policy.

5.2 Access to social networks

Many organisations permit staff to access the Internet for ‘private-purposes’, and in the author’s opinion this number is likely to increase as more of our daily lives are conducted ‘on-line’. There will of course be constraints in terms of for example, time spent browsing (max.), ‘blocked’ versus ‘unblocked’ sites, and restrictions on content-types that may be downloaded. Access to social networking sites, with the exception of the applications / widgets should not be blocked.

Social networking sites also have the potential to benefit business, and as above, access to access to social networking sites, with the exception of the applications / widgets should not be blocked.

5.3 Information content – Guidelines

Staying safe on a social networking service means working knowledgeably within a set of simple guidelines.

- **Be Discreet** - Assume that the Social networking site is susceptible to compromise and never type anything of a ‘sensitive’ nature. For example, phone numbers, job titles, birth dates, schedule details and daily routines.
- **Be Skeptical** - Treat anything you see online with a high degree of skepticism, for example, stock tips, advance news, personnel gossip and so on
- **Be Thoughtful** - Never type anything online that can come back to bite you. For example, outrageous claims, slander, obscenity and insults
- **Be Professional** - If you're posting a picture or video to a social network site, make sure it presents you in the best possible light.
- **Be Wary** - People on the Internet are not always who they seem to be. The CEO you're chatting with in Denver may actually be a 14-year-old kid in Romania.

- **Check Privacy Policies** - All major social network services have specific privacy guidelines that are published on their Web sites. Take the time to read and understand these documents, since they include the types of information that they will reveal or sell to other parties (including spammers). If you don't like the terms, don't use the service.

5.4 End-user devices

Anti-virus software should be hosted on end-user devices which are at risk from the import of malicious code. Note risks vary significantly depending on the operating system and type of device:

Details	**Risk**
Desktop / laptops	Windows – very high Linux– low Apple –medium[11]
Tablet / Smart phones	Generally speaking the risk is still 'low', however as and when greater functionality is incorporated in the device, so the threat from the writers of malicious code will increase. For example, as smart phones and PDAs develop new capabilities, such as the capacity to work with scripting languages, they will become more susceptible to Trojan horses, viruses, and worms."

5.5 Corporate network

Anti-virus and content checking software shall be deployed at the perimeter of corporate networks to protect against the import of malicious code via web-browsing.

Anti-virus software shall be hosted on corporate networking sites.

[11] See article "http://www.pcworld.com/article/208540/mac_users_warned_of_growing_virus_threat.html"

5.6 Applications

5.6.1 Desktop applications - Guidance

Do not download desktop applications by following links provided in Internet-based social networking sites.

Only download applications from Trusted sources, and even then seek advice and authorisation from the IT department[12]. Furthermore:

- Personal Smart phones with access to the corporate network (e.g. email, calendar and contacts) shall adhere to the same security rules which apply to corporate assets.
- The IT department shall maintain a list of 'trusted' applications, based on the use of reputable suppliers, advice from Government and industry experts, and its own research, for example Google searches for 'known' security threats / risks.

End-user devices shall be configured to restrict the download feature to IT administration staff, wherever possible, including workstations, laptops, tablet devices and Smart phones[13]

5.6.2 Browser-based applications - Guidance[14]

Internet sites

Do not 'accept' invitations to use browser-based applications available on Internet-based social networking sites, e.g. games, quiz.

Corporate sites

Browser-based applications to be accessible from corporate social networking sites shall be reviewed before being released.

Invitations to use browser based applications on corporate social networking sites may be 'accepted'.

---

[12] It is not difficult to get iPhone apps approved, Nicolas Seriot said. To get an app distributed through Apple's App Store, developers need to be enrolled in the iPhone Developer Program and provide an executable file, but not the source code, to Apple for vetting. The approval process mainly looks for user interface inconsistencies, but also undocumented function calls and malware, he said. But with Apple having to scrutinize as many as 10,000 binaries that are submitted each week, some malware is bound to sneak in, Seriot said. He acknowledged that he doesn't know exactly what process Apple uses to review apps but said it likely uses common static and dynamic analysis, both of which can be circumvented with the right programming tricks, he said.

[13] E.g. Blackberry feature.

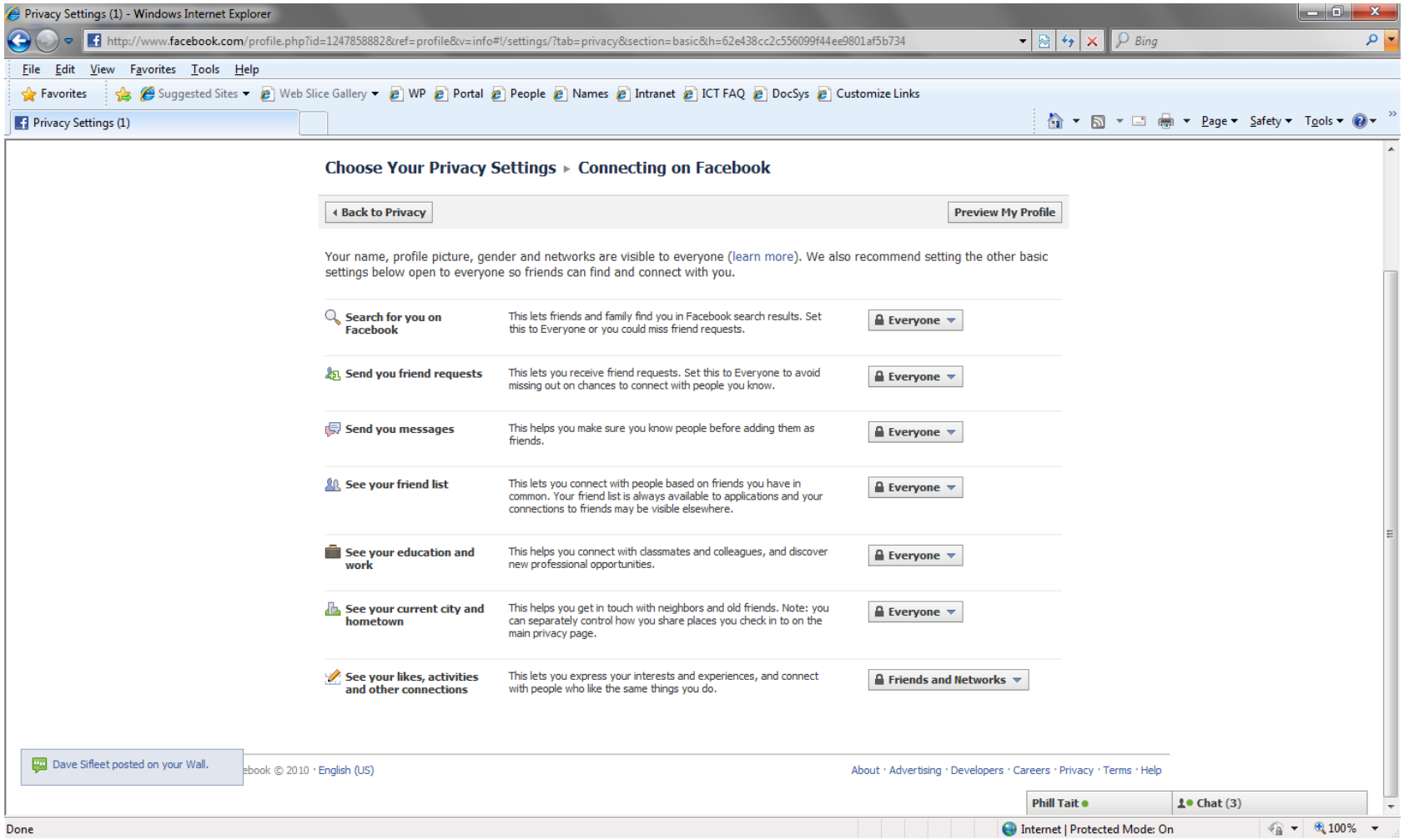
[14] Review the application and the site from which a proposed download is to be made.

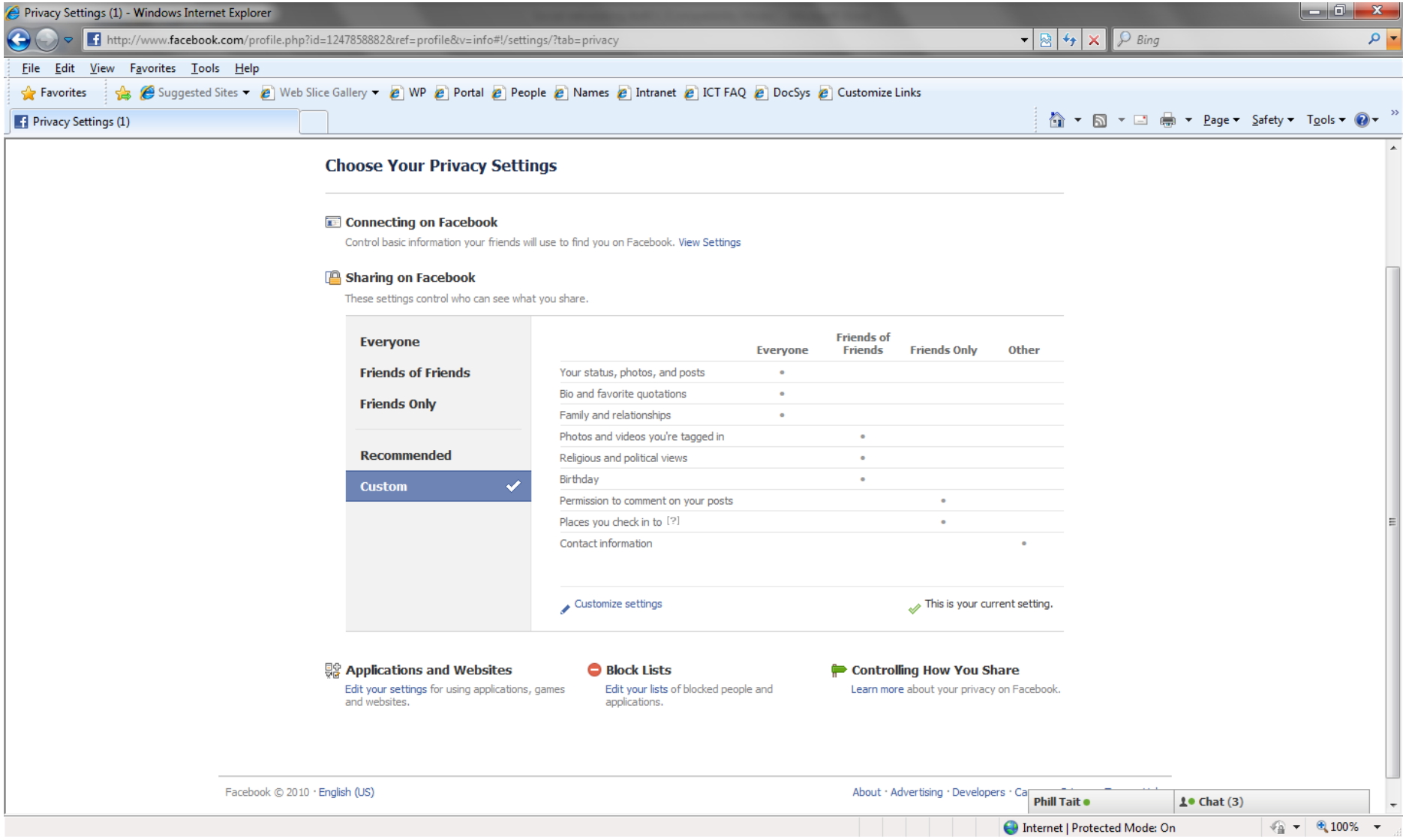
6 Recognition

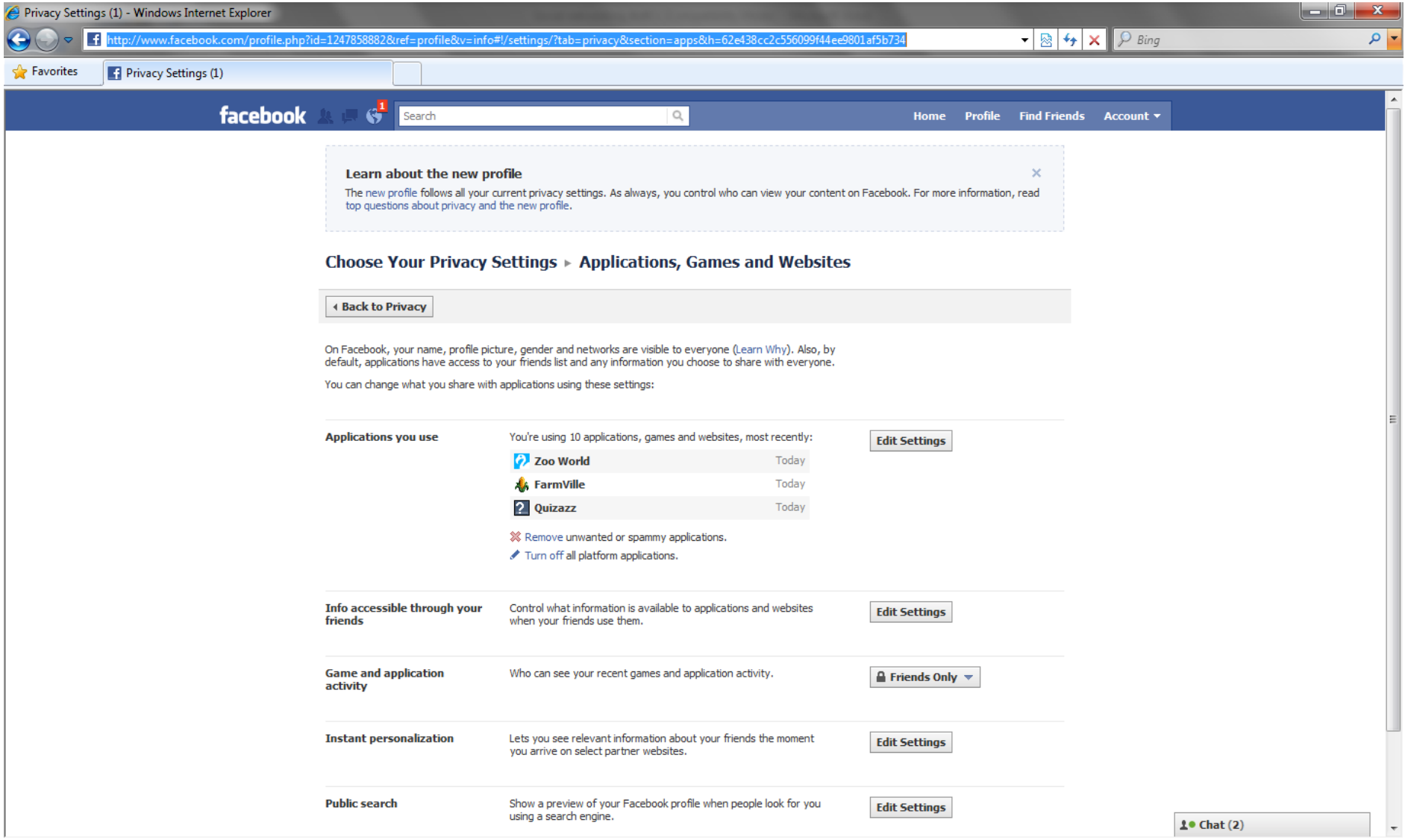
The author would like to thank Edward Hamilton (from Analysys Mason) for his contribution during the production of this whitepaper.

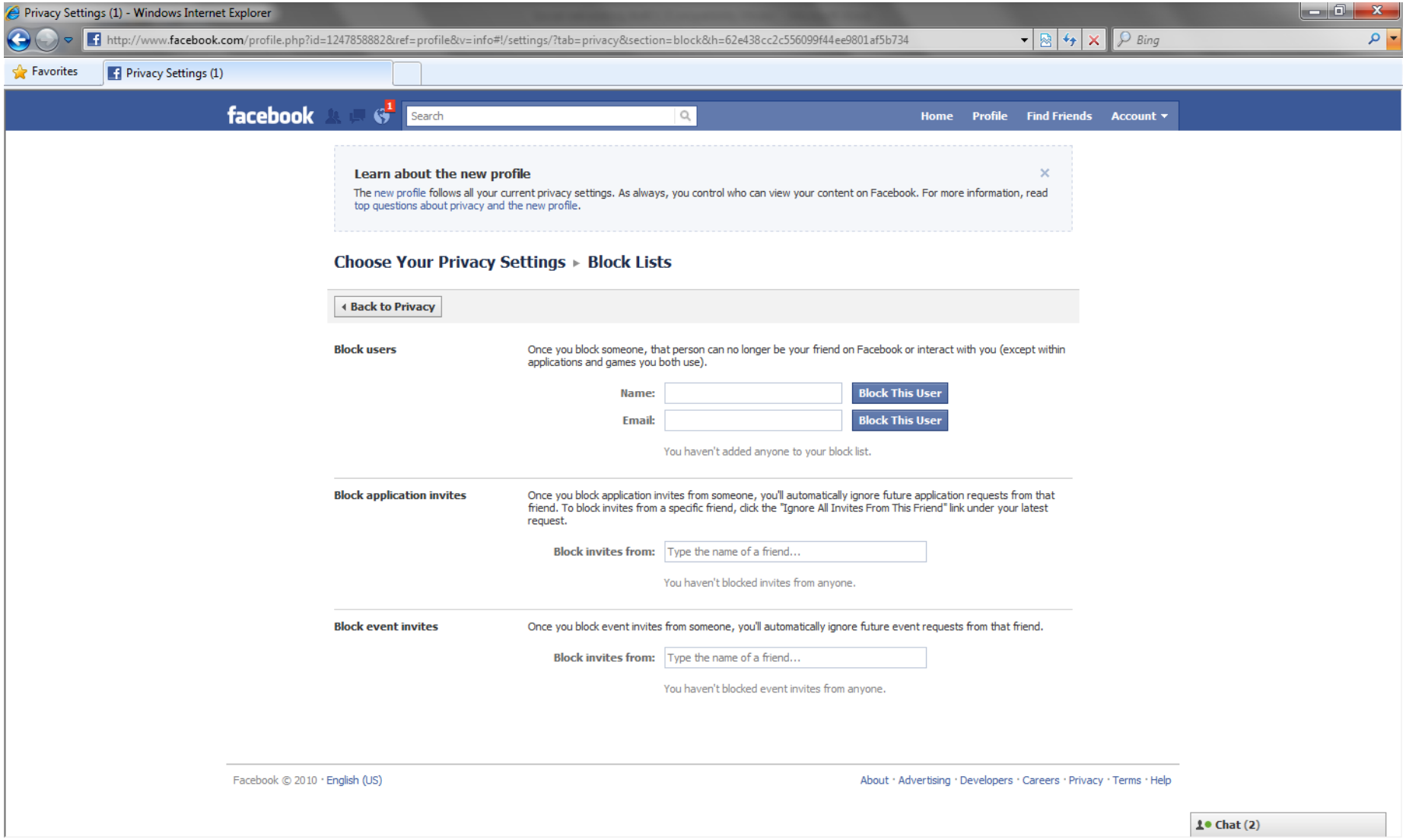
In addition the author would like to thank the many individuals who have uploaded papers on social networking to the Internet.

Annex A: Privacy settings




Privacy Settings (1) - Windows Internet Explorer
http://www.facebook.com/profile.php?id=1247858882&ref=profile&v=info#!/settings/?tab=privacy
Bing
File Edit View Favorites Tools Help
Favorites Suggested Sites Web Slice Gallery WP Portal People Names Intranet ICT FAQ DocSys Customize Links
Privacy Settings (1)
Page Safety Tools
Choose Your Privacy Settings
Connecting on Facebook
Control basic information your friends will use to find you on Facebook. View Settings
Sharing on Facebook
These settings control who can see what you share.
Everyone
Friends of Friends
Friends Only
Recommended
Custom
Everyone
Friends of Friends
Friends Only
Other
Your status, photos, and posts
Bio and favorite quotations
Family and relationships
Photos and videos you're tagged in
Religious and political views
Birthday
Permission to comment on your posts
Places you check in to [?]
Contact information
Customize settings
This is your current setting.
Applications and Websites
Edit your settings for using applications, games and websites.
Block Lists
Edit your lists of blocked people and applications.
Controlling How You Share
Learn more about your privacy on Facebook.
Facebook © 2010 · English (US)
About · Advertising · Developers
Phill Tait
Chat (3)
Internet | Protected Mode: On
100%


Privacy Settings (1) - Windows Internet Explorer
http://www.facebook.com/profile.php?id=1247858882&ref=profile&v=info#!/settings/?tab=privacy&section=apps&h=62e438cc2c556099f44ee9801af5b734
Bing
Favorites
Privacy Settings (1)
facebook
Search
Home
Profile
Find Friends
Account
Learn about the new profile
The new profile follows all your current privacy settings. As always, you control who can view your content on Facebook. For more information, read top questions about privacy and the new profile.
Choose Your Privacy Settings ▸ Applications, Games and Websites
Back to Privacy
On Facebook, your name, profile picture, gender and networks are visible to everyone (Learn Why). Also, by default, applications have access to your friends list and any information you choose to share with everyone.
You can change what you share with applications using these settings:
Applications you use
You're using 10 applications, games and websites, most recently:
Zoo World Today
FarmVille Today
Quizazz Today
Remove unwanted or spammy applications.
Turn off all platform applications.
Edit Settings
Info accessible through your friends
Control what information is available to applications and websites when your friends use them.
Edit Settings
Game and application activity
Who can see your recent games and application activity.
Friends Only
Instant personalization
Lets you see relevant information about your friends the moment you arrive on select partner websites.
Edit Settings
Public search
Show a preview of your Facebook profile when people look for you using a search engine.
Edit Settings
Chat (2)


Privacy Settings (1) - Windows Internet Explorer
http://www.facebook.com/profile.php?id=1247858882&ref=profile&v=info#!/settings/?tab=privacy&section=block&h=62e438cc2c556099f44ee9801af5b734
Bing
Favorites
Privacy Settings (1)
facebook
Search
Home
Profile
Find Friends
Account
Learn about the new profile
The new profile follows all your current privacy settings. As always, you control who can view your content on Facebook. For more information, read top questions about privacy and the new profile.
Choose Your Privacy Settings ▸ Block Lists
Back to Privacy
Block users
Once you block someone, that person can no longer be your friend on Facebook or interact with you (except within applications and games you both use).
Name:
Block This User
Email:
Block This User
You haven't added anyone to your block list.
Block application invites
Once you block application invites from someone, you'll automatically ignore future application requests from that friend. To block invites from a specific friend, click the "Ignore All Invites From This Friend" link under your latest request.
Block invites from:
Type the name of a friend...
You haven't blocked invites from anyone.
Block event invites
Once you block event invites from someone, you'll automatically ignore future event requests from that friend.
Block invites from:
Type the name of a friend...
You haven't blocked event invites from anyone.
Facebook © 2010 · English (US)
About · Advertising · Developers · Careers · Privacy · Terms · Help
Chat (2)