A Survey on Social Network Sites for Security

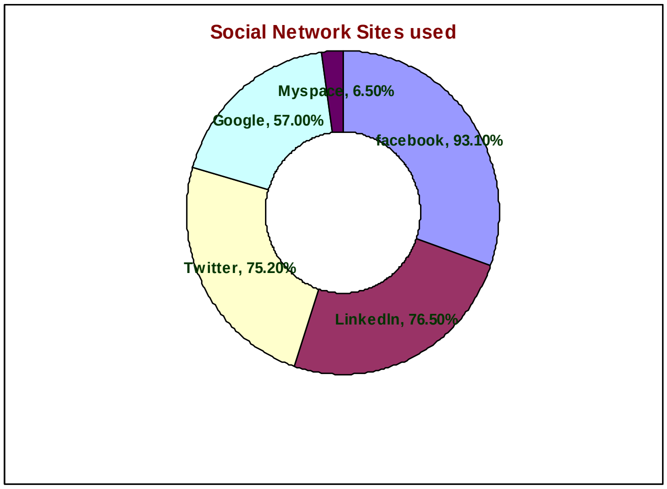
Dr. K. Nirmala, N. Zackariah

Abstract -Internet Social Networks are great places to meet and network with people sharing similar business interests. But MySpace, Second Life and similar Web 2.0 sites can also pose serious security threats to users and their companies. Many businesses view social networking sites as a kind of online cocktail party -- a friendly, comfortable place where one can establish contacts, find buyers or sellers, and raise a personal or corporate profile. But the cocktail party metaphor isn't entirely accurate. In fact, users would be better served if they thought of social network services in the context of a loud glass house; a place with endless visibility and each occupant talking through a highly amplified bullhorn. Since most people access social network sites from the comfort and privacy of their home or office, they can be lulled into a false sense of anonymity. Additionally, the lack of physical contact on social network site can lower users' natural defences, leading individuals into disclosing information they would never think of revealing to a person they just met on a street -- or at a cocktail party's.

Index Terms – Social Networks, MySpace, Web 2.0, Facebook, Cocktail party

1. INTRODUCTION

Social Networks have become part of the business and personal fabric of the world [1]. About a billion people use various social networks around the world to engage in personal relationships and to conduct business. This growth and advancement faces risks of attackers targeting users as well as users concerns about personal privacy.



1.1 Security Threats

Social media platforms such as Twitter, Facebook and LinkedIn increasingly are being used by enterprises to engage with customers, build their brands and communicate information to the rest of the world. But social media for enterprises isn't all about "liking," "friending," "up-voting" or "digging." For organizations, there are real risks to using social media, ranging from damaging the brand to exposing proprietary information to inviting lawsuits. The following six threats are generally faced in a business.

2 MOBILE APPLICATIONS

The rise of social media is inextricably linked with the revolution in mobile computing, which has spawned a huge industry in mobile application development. Naturally, whether using their own or company-issued mobile devices, employees typically download dozens of applications because, well, because they can. Social networking security threats taken too lightly. But sometimes they download more than they bargained for. Some of the malware was designed to reveal the user's private information to a third party, replicate itself on other devices, destroy user data or even impersonate the device owner.

2.1 Social engineering

A favorite of smooth-talking scammers everywhere, social engineering has been around since before computer networks. But the rise of the Internet made it easier for grifters and flim-flam artists to find potential victims who may have a soft spot in their hearts for Nigerian royalty. Social media has taken this

- Associate Professor, Department of Computer Science, Quid-E-Millath Govt. College for Women, Chennai, Tamilnadu, India-600002. .E-mail: nimimca@yahoo.com
- Research Scholar, Bharathiar University, Coimbatore, Tamilnadu. India. E-mail: n.zackariah@gmail.com

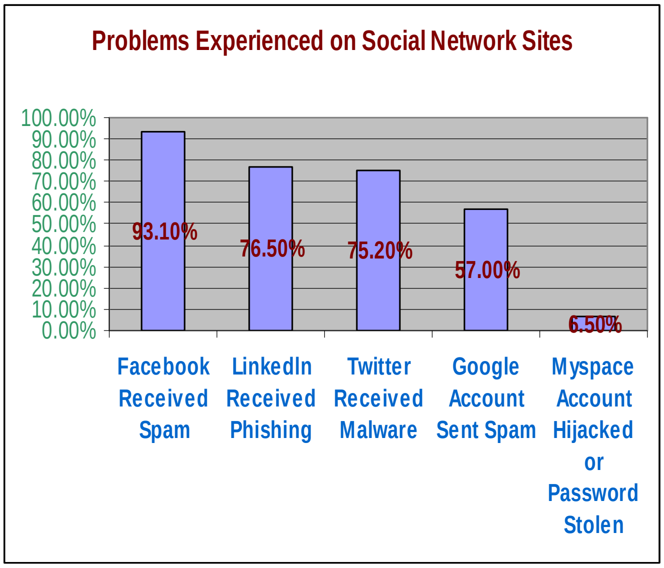
threat to a new level. People are more willing than ever to share personal information about themselves online via Facebook, Twitter, Foursquare and Myspace, and social media platforms encourage a dangerous level of assumed trust.

2.2 Social networking sites

Sometimes hackers go right to the source, injecting malicious code into a social networking site, including inside advertisements and via third-party apps. On Twitter, shortened URLs (popular due to the 140-character tweet limit) can be used to trick users into visiting malicious sites that can extract personal (and corporate) information if accessed through a work computer. Twitter is especially vulnerable to this method because it's easy to retweet a post so that it eventually could be seen by hundreds of thousands of people.

2.3 Our employees

Some times, even the most responsible employees have lapses in judgment, make mistakes or behave emotionally. Nobody's perfect all of the time. But dealing with an indiscreet comment in the office is one thing; if the comment is made on a work-related social media account, then it's out there, and it can't be retrieved. Remember, this wasn't some low-level employee not tuned into the corporate mission. This was a high-level communications executive who damaged his company's brand and endangered an account. Imagine what a disgruntled low-level employee without as much invested in his job might be able to do with social media tools and a chip on his shoulder.



2.4 Lack of a social media policy

Without a social media policy for an enterprise, we are inviting disaster. We can't just turn employees loose on social networking platforms and urge them to "represent." We need to spell out the goals and parameters of our enterprise's social media initiative. Otherwise we'll get exactly what we're inviting will be problems.

3 PROTECT THE BUSINESS

The following ideas can be used for protect our business from the external threats. Be Discreet : Never type anything into a profile page, bulletin board, instant message or other type of online electronic form that would expose you to unwanted visitors or the possibility of identity theft or malicious threats. This includes personal and business names and addresses, phone numbers, job titles, birth dates, schedule details, daily routines and business or family information. It's far better to communicate in generalities than to reveal information that unscrupulous individuals may someday use against you. Be Skeptical : Social network sites are full of useful business information, as well as to substantial amounts of useless disinformation. Treat anything you see online -- stock tips, advance news, personnel gossip and so on -- with a high degree of skepticism. Some people will lie in order to boost their own agenda, while others will spout unsubstantiated rubbish out of stupidity or sheer ignorance. Be Thoughtful : Nobody likes a loudmouth, but the Internet has a curious way of releasing personal inhibitions. Never type anything online that can come back to bite you. This includes outrageous claims, slander, obscenity and insults. Be cool and professional, and always think twice before typing. 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. Dress professionally and, above all, don't disrobe or wear a funny hat. 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 Milwaukee -- or a prisoner in Romania. Until you can independently verify someone's identity -- using the same business tools that you would turn to to screen a new hire or confirm a prospective business partner -- never, ever reveal personal, business or financial information. 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.

4. TIPS FOR SOCIAL NETWORKING SAFETY

Social networking websites like MySpace, Facebook, Twitter, and Windows Live Spaces are services people can use to connect with others to share information like photos, videos, and personal messages. As the popularity of these social sites grows, so do the risks of using them. Hackers, spammers, virus writers, identity thieves, and other criminals follow the traffic. The following tips to help protect when use social networks.

4.1 Use caution when click links

some times the received mails contain treat links in messages. Clicking such a links should be avoided.

4.2 Know what to be posted:

A common way that hackers break into financial or other accounts is by clicking the "Forgot your password?" link on the account login page. To break into your account, they search for the answers to your security questions, such as your birthday, home town, high school class, or mother's middle name. If the site allows, make up your own password questions, and don't draw them from material anyone could find with a quick search.

4.3 Don't trust that a message is really from who it says it's from

Hackers can break into accounts and send messages that look like they're from your friends, but aren't. If you suspect that a message is fraudulent, use an alternate method to contact your friend to find out. This includes invitations to join new social networks.

4.4 To avoid giving away email addresses of your friends

Do not allow social networking services to scan your email address book. When you join a new social network, you might receive an offer to enter your email address and password to find out if your contacts are on the network. The site might use this information to send email messages to everyone in your contact list or even everyone you've ever sent an email message to with that email address. Social networking sites should explain that they're going to do this, but some do not.

4.5 Type the address of your social networking site directly into your browser or use your personal bookmarks

If you click a link to your site through email or another website, you might be entering your account name and password into a fake site where your personal information could be stolen.

4.6 Be selective about who you accept as a friend on a social network

Identity thieves might create fake profiles in order to get information from you.

4.7 Choose your social network carefully

Evaluate the site that you plan to use and make sure you understand the privacy policy. Find out if the site monitors content that people post. You will be providing personal information to this website, so use the same criteria that you would to select a site where you enter your credit card.

4.8 Assume that everything you put on a social networking site is permanent

Even if you can delete your account, anyone on the Internet can easily print photos or text or save images and videos to a computer.

Be careful about installing extras on your site: Many social networking sites allow you to download third-party applications that let you do more with your personal page. Criminals sometimes use these applications to steal your personal information. To download and use third-party applications safely, take the same safety precautions that you take with any other program or file you download from the web. Think twice before you use social networking sites at work & Talk to your kids about social networking

5. CONCLUSION

Social network sites are potentially useful business tools, but only if you approach them with an adequate amount of caution and common sense. It’s clear that businesses need a proactive— and powerfully persuasive—communications plan to educate their user community about social media risks, personal and company impacts, and expected behaviors. Companies should support the communications plan with targeted protections to mitigate the risks of social networking, a phenomenon that will only continue to gain force.

REFERENCES

[1] Dr. Paul Judge,2011, *Social Networking Security and Privacy Study.*

[2] http://www.networkworld.com/news/2011/053111-social-media-security.html?page=2

[3] http://www.microsoft.com/security/online-privacy/social-networking.aspx

[4] http://www.networkworld.com/news/2011/053111-social-media-security.html?page=1

[5] Gary Loveland, , May 2009,*Secure Enterprise 2.0 Forum, Q1 2009 Web 2.0 Hacking Security Report.*