Social Media Security Risk and It’s Protection against Security Attacks

Dr. Ateeq Ahmad
Jyoti Group of Education, Bareilly, U.P., India

Abstract
Social Media Security is one of the most pressing Information Technology issues that any business faces today, but it’s especially a concern for small and mid-sized companies who find it difficult and increasingly complex to find the resources needed to protect against the ever growing number of security risk. 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. For organizations, there are real risks to using social media, ranging from damaging the brand to exposing proprietary information. The basic aim of this article is to protecting the system against unauthorized social media attack.

Key words:
Security Risk, Security Attack, Social Media, Social Network.

1. Introduction
Social media marketing presents attractive options for small businesses with limited time and resources. It’s cute at first but it can grow to strangle you. It can be hard for a time starved small business to keep peace and know what to do when it comes to connecting with customers and members on sites like Facebook, Twitter, LinkedIn, Foursquare, and other specialty social networks. Add to it the safety, security, privacy, and reputation threats of social media from the perspective of having to support your small business’s social media efforts and you get the perfect storm. Trying to get entrepreneurial risk takers to move into Social Media Risk Management.

A recent study courtesy of Internet security company Panda Labs in its “2010 Annual Security Report” of the world’s most popular social media sites determined that social media sites are a “perfect working environment” for cybercriminals because Internet users, for now, place more trust in these sites than other online tools, like email. And they identified Facebook and Twitter as being the most affected by security breaches and shared some of the tricks these cybercriminals use in gaining access to your account such as hijacking Facebook’s “Like” button, stealing identities to send out messages from trusted sources, exploiting vulnerabilities in Twitter to run JavaScript code, distributing fake apps that redirect users to infected sites, and so on. The report went on to state “In 2011, not only will hackers continue to use these networks, but it is predicted that they will also be used more for distributed attacks.” They seemed to have had a crystal ball. If you are a social media marketer, you are losing everything. Not only your reputation; but also your safety, security, and privacy. If you trust your intuition Granted Twitter, Facebook and other social media sites are great ways to communicate and to do marketing. Nevertheless, if you’re not careful they can open the door to serious risks. Running a small business requires weighing the various risk types you face as well as resource limitations and complex value propositions, and then making decisions about where to place your attention and resources.

Attacks from social media use include malware infection, identify theft, data loss and reputation damage both to users and their small businesses. Increased use of social media for marketing purposes together with demands for greater access within small businesses mean increased safety, security, privacy, and reputation concerns. Even home use can have implications for a small business through revealing sensitive information. It's vital to inform your users about the threats from social media.

2. Definition
Social media includes web based and mobile technologies used to turn communication into interactive dialogue.

Social media is all about leveraging online tools that promote sharing and conversations, which ultimately lead to engagement with current and future customers and influencers in your target market. The key to social media working, is having a content marketing strategy that involves the distribution of valuable, relevant and compelling content that promotes the behavior you are looking for that will ultimately drive your business. Most businesses start with the tools. Effective social media
starts with a content strategy that helps to position you and your brand as the expert in your niche through provocative, informative and helpful content. Then, once that is accomplished, the social media tools are now available today that make the plan come together. (Joe Pulizzi)

Social media as “a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content (Andreas Kaplan and Michael Haenlein).

Social media is media for social interaction as a super-set beyond social communication. Enabled by ubiquitously accessible and scalable communication techniques, social media has substantially changed the way organizations, communities, and individuals communicate (Kietzmann, Jan H.; Kris Hermkens, Ian P. McCarthy, and Bruno S. Silvestre -2011).

3. Objectives

The main purpose of this article is to learn the tools and motives involved in social media attacks and share the lesson with the learners, those who are involved in research related to security risk of social media.

4. Importance of Social Media Security Risk

Social Media security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done.

5. Social Media Security Attacks.

Boundaries between personal and work life are falling away and we increasingly use social media, in fact growing percent of the time we spend online, putting pressure on security. Clear guidance is needed for employees to make sure security standards are set and that the personal as well as business risks are known and avoided.

Managing editor for news, Computerworld predicts for 2012 that: “It’s only a matter of time before some big-name company loses important corporate data because of the failure to secure these personal devices.” (Ken Mingis,)

Online Social media security risks are relentlessly inventive. Masters of disguise and manipulation, these threats constantly evolve to find new ways to annoy, steal and harm. Arm yourself with information and resources to safeguard against complex and growing Social media security threats and stay safe online. There are some common threats that are attacking to the social media.

5.1 Virus Attack

A computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user. A virus replicates and executes itself, usually doing damage to your computer in the process.

5.2 Spyware Attack

Spyware is a program that monitors your online activities or installs programs without your consent for profit or to capture personal information. We’ve amassed a wealth of knowledge that will help you combat spyware threats and stay safe online.

5.3 Hackers Attack

People, not computers, create computer security threats and malware. Hackers are programmers who victimize others for their own gain by breaking into computer systems to steal, change or destroy information.

5.4 Phishing Attack

Phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Internet Based attacks While your computer is connected to the Internet it can be subject to attack through your network communications.

5.5 Viral Web Sites Attack

Users can be enticed, often by email messages, to visit web sites that contain viruses or Trojans. These sites are known as viral web sites and are often made to look like well known web sites and can have similar web addresses to the sites they are imitating. Users who visit these sites often inadvertently download and run a virus or Trojan and can then become infected or the subject of hacker attacks.

5.6 Adware, Advertising and Trojans Attack

Adware, Advertising and Trojans are often installed with other programs, usually without your knowledge. They record your behaviors on the Internet, display targeted ads to you and can even download other malicious software on to your computer. They are often included within programs that you can download free from the Internet.
5.7 Spyware Attack
Spyware doesn’t usually carry viruses but it can use your system resources and slow down your Internet connection with the display of ads. If the Spyware contains bugs it can make your computer unstable but the main concern is your privacy. These programs record every step that you take on the Internet and forward it to an Ad Management Centre which reviews your searches and downloads to determine your shopping preferences. The Ad Management Centre will build up a detailed profile of you, without your knowledge, and can pass this on to third parties, again without your knowledge. Some Spyware can download more serious threats on to your computer, such as Trojan Horses.

5.8 Unsecured Wireless Access Points Attack
Wireless access point, e.g. an ADSL (Broadband) Router, hasn't been secured then anyone with a wireless device (laptop, PDA, etc) will be able to connect to it and thereby access the Internet and all the other computers on the wireless network.

5.9 Bluesnarfing Attack
The act of stealing personal data, specifically calendar and contact information, from a Bluetooth enabled device.

5.10 Social Engineering Attack
A favorite of smooth-talking scammers everywhere, social engineering has been around since before computer networks. Tricking computer users into revealing computer security or private information, e.g. passwords, email addresses, etc, by exploiting the natural tendency of a person to trust or by exploiting a person's emotional response.

5.11 Mobile Application Attack
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.

5.12 Social networking websites Attack
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 can be used to trick users into visiting malicious sites that can extract personal 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.

5.13 Employees Mistakes
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.

6. System Protection against Attacks
Need to implement and enforce an acceptable usage policy covering the use of social media sites. The best way to ensure your policy works is to develop it through consultation with your employees and strictly enforce it. Employees are less likely to circumvent restrictions if they understand the logic behind them and have been involved in developing the overall policy. social networking security best practice to permit access only to social networking sites that have obvious business benefits and only to users with a business need to access them. When deciding which sites employees are allowed to access, you should take into account the sites' terms and conditions, as well as what they can do with user information and content. It is key that all staff receive security awareness training covering your acceptable usage policy for social networking. Promoting good practice and improving user behavior are the best methods of reducing the risks from this form of communication. Many social networking sites' profile pages encourage the publication and sharing of personal information, but it can be harvested and used for phishing or targeted malware attacks against the user or organization, possibly putting personnel safety and the organization's information assets and reputation at risk. Employees need to be made aware that although content can easily be posted, it is essentially impossible to completely delete it. User training should also cover the common social network malware scams and social engineering techniques used to procure personal or login information. Of course the use of strong passwords should be mandated and, where possible, require users to operate separate personal and work accounts. Also, advise users to make full use of any available privacy settings that control what information is viewable and to whom.
These are all good practices, but making your security policies enforceable will have a much bigger effect on your users' overall behavior. Web monitoring tools, such as Websense Inc.’s Web Security Gateway, or BlueCoat Systems Inc.’s ProxyAV line, can detect holes in your acceptable usage policy so it can be updated or, when necessary, disciplinary steps can be taken against specific users. Also, data loss prevention tools can prevent accidental or intentional data disclosures via social networking by analyzing content. File access and blocking inappropriate access or transmission, while warning users at the same time. Except this there are some common method is also use for preventing the system.

6.1. Protection from Threats Attack

- Recovering from Viruses, Worms, and Trojan Horses
- Avoiding Social Engineering and Networking Attacks
- Avoiding the Pitfalls of Online Trading
- Using Caution with USB Drives
- Securing Wireless Networks

6.2. Protection from Email Communication

- Using Caution with Email Attachments
- Reducing Spam
- Using Caution With Digital Signatures
- Using Instant Messaging and Chat Rooms Safely
- Staying safe on social Network Sites

6.3. Protection from Browsing

- Evaluating Your Web Browser's Security Settings
- Shopping Safely Online
- Web Site Certificates

6.4. Privacy Control and Others Protection

- Protecting Your Privacy
- Effectively Erasing Files
- Supplemeting Passwords
- Install and Use Anti-Virus Programs
- Use Care When Reading Email with Attachments
- Install and Use a Firewall Program
- Make Backups of Important Files and Folders
- Use Strong Passwords
- Use Care When Downloading and Installing Programs
- Install and Use a Hardware Firewall
- Install and Use a File Encryption Program and Access Controls
- Safeguard your Data
- Real-World Warnings keep you safe online.
- Keeping Children Safe Online

Conclusion

A few years ago, due to resource limitations, risk assessments, and time restrictions, it may have been impractical to deploy security of Social media. However, the risks and time involved with deploying security of Social media are minimal when using current technology. Thus it is the conclusion of this article that a Social media can be implemented and protected by using various security tools.

References


