



## Social Network Services – Your Connected Threat

### **Overview**

Social network services are used by individuals and organizations to meet, establish, and maintain relationships with others. In business, sales departments use social network services to convey information about new products and services and to solicit customer feedback. What many people don't know, however, is that social network services can create risks to the individual and your organization.

Social network services are web sites on the Internet that allow sharing of information between friends, relatives, and business contacts. The process of developing relationships has become easier through web sites such as Facebook, Flickr, Foursquare, LinkedIn, Myspace, Twitter, and others. These applications make it easy to post information about your daily life and work. However, these same sites raise privacy and security concerns.

Social network services are similar to traditional web applications and have some of the same types of threats. Social network services are vulnerable to traditional malicious software (malware), spam, social engineering, and similar threats. In addition, an organization may be vulnerable to threats related to the disclosure of sensitive information or intellectual property.

Social network services have taken some steps to protect their customers, but they can't protect against all risks.

### **Intelligent malware**

Modern malware is more intelligent than the malicious software used in the past. With social networks, malware typically uses browser based vulnerabilities to infect a victim's computer system. In many instances, hyperlinks are used to embed malicious content in social network profiles and pages. When a user visits an infected page, the malware analyzes the visitor's browser and version number and delivers the appropriate exploit. This helps ensure compatibility with the victim's computer. The malware has a greater chance of being undetected and offers the hacker a greater chance of success at compromising the victim's computer system.

### **Identity theft**

If you don't own your own and control your own profile, it is relatively easy for someone to use the Internet to collect enough information about you or your business and create a fake identity. The fake profile is then used to communicate with others, often tempting them to visit your page. A hacker then uses the profile to commit identity theft or embeds malicious code that infects users that have visited the fake profile.



### **Social engineering risks**

Hackers use a combination of social engineering and social network services to infect computer systems. A hacker sends a phishing (fake) e-mail to selected individuals. When an individual opens the message and clicks on an html link, the individual is delivered to your fake social media page. The fake page entices the individual to click on a link to a new site that contains music files. When the individual clicks on the link to the music file, the music plays while malicious software is downloaded to their computer.

### **Pyramid scheme risks**

Hackers turn social networking features to their advantage. Social network services were designed to facilitate the sharing of information and hackers leverage this to their advantage, using the network to launch attacks against others. Once one person's computer is compromised, it can be used to connect with, and infect, other computer systems.

In the pyramid scheme, hackers target heavy users of social networking sites. By exploiting browser vulnerabilities, hackers place malware on a victim's computer. The victim is the first level of the pyramid. The malware opens a backdoor and allows a hacker full access to the computer. The computer is turned into a zombie where it tracks the user's activity and waits for the victim to log into a social networking site. Once logged in, the malware secretly starts posting messages to infect the social networking contacts of the user (the second level of the pyramid). Once infected, the process repeats as the second level contacts are turned into zombies that load malware on third and fourth level contacts. The process continues as it infects more and more computer systems.

### **Custom programming risks**

Application Programming Interfaces (API) facilitate the interaction between various software programs. With social network services, API's are used to extend the features of the software with graphs, photos, ads, etc. However, API's can also be used by hackers to conduct sophisticated attacks that use JavaScript to solicit personally identifiable information from visitors to the page.

### **Information disclosure risks**

Information posted on the Internet may exist for a long time. Not only it is posted on web site pages, but it may be archived on backup tapes and other media. A good rule of thumb is that you shouldn't post anything you wouldn't want to read in the front page of your local newspaper.



## 10 Steps to protect against social network threats

In a virtual environment you don't have a strong real world connection to others. Take the following steps to protect against social networking risks:

1. *Settings* – to protect your privacy, apply the appropriate restrictions and settings provided by the social network services. Monitor social network privacy changes and features. Change privacy settings to “friends only” so that hackers cannot see your profile.
2. *Security awareness* – educate yourself and your staff on the dangers of clicking on links in text messages and e-mail. Know how to detect false profiles and fake e-mail messages.
3. *Friends* - take care when accepting friend requests in case the profiles in question are fakes. Most hackers don't have time to create long and interesting profiles. Also, it is probably a fake if they have lots of friends and have only had a profile a short amount of time.
4. *Claim your name* - create your own social network profile on the major sites before they can be claimed by imposters.
5. *Disclosure* – revealing too much information about yourself or your organization creates risks. Remove any sensitive information you do not want disclosed to others. Organizations should implement social networking policies dictating who in your organization is permitted to post information, the type of information that can be posted, how it is to be managed, and how the organization's on-line social identity and intellectual property will be protected.
6. *Smartphones* – in many cases the phone has been programmed with the password to social networking sites. This makes it easy for the phone user but also makes it easy for a hacker. Ensure your phone has a password lock.
7. *Protection software* – ensure all devices used to access social network services have malware protection. This includes anti-virus and anti-spyware protection. Some protection software includes the ability to remotely wipe a smartphone if it is lost or stolen.
8. *Patch management* – ensure your application, operating system, third party software (pdf readers, flash, etc.), and web browsers are patched and updated on a regular basis.
9. *Incident response* – notify social network security teams if you detect suspicious activity. The security teams can remove infected pages and apply filters to restrict future activity.
10. *Privacy policy* – read and understand the privacy policy posted on the social network service. If you don't agree to their terms, don't use their service.



## **Summary**

Social network services are similar to traditional web applications and have some of the same types of threats. Social network services are vulnerable to traditional malicious software (malware), spam, social engineering, and similar threats. In addition, an organization may be vulnerable to threats related to the disclosure of sensitive information or intellectual property.

Social network services have taken some steps to protect their customers, but they can't protect against all risks. Formal risk assessments and audits help organizations identify, manage, and reduce their risks.

## **Publication and Author Information**

Jim Kelton is Managing Principal of Altius IT ([www.AltiusIT.com](http://www.AltiusIT.com)), an IT security audit, security consulting, and risk management company based in Costa Mesa, California. Mr. Kelton has over 30 years of experience in the Information Technology industry and is recognized as a security expert. He is certified by the Information Systems Audit and Control Association (ISACA) as:

Certified Information Systems Auditor (CISA)

Certified in Risk and Information Systems Controls (CRISC)

Certified in the Governance of Enterprise IT (CGEIT)

He sits on the Board of Directors of the following associations and organizations:

- Association of Professional Consultants (APC)
- International Association of Professional Security Consultants (IAPSC)
- Technology Professionals Association (TPA)