Journal of Strategic Security

Volume 3
Number 2 *Volume 3, No. 2: Summer 2010*

Article 7

The Weakest Link: The Risks Associated with Social Networking Websites

Yosef Lehrman
New York Police Department, ylehrman@gmail.com

pp. 63-72

Recommended Citation
Lehrman, Yosef. "The Weakest Link: The Risks Associated with Social Networking Websites." *Journal of Strategic Security* 3, no. 2 (2010) : 63-72.
DOI: http://dx.doi.org/10.5038/1944-0472.3.2.7
Available at: https://digitalcommons.usf.edu/jss/vol3/iss2/7

The Weakest Link: The Risks Associated with Social Networking Websites

Abstract

The relatively rapid rise in popularity of social networking services is now well known. MySpace, Twitter, and Facebook have become well known sites and terms. According to the Web traffic tracking site Alexa.com, as of December 2009, Facebook had 350 million registered users, MySpace just under 475 million, and Twitter 44.5 million. Many people think very little of posting prodigious amounts of personal information on social networking sites, not realizing that this information puts them at risk. Specifically, those in the law enforcement and military communities may not realize that information posted on these sites can compromise operational security and potentially endanger lives. In July 2009, the Associated Press ran a story which was picked up by most major news outlets in the USA, in which it was reported that the wife of the incoming head of Britain's MI6 intelligence agency had posted pictures and family details on her Facebook page. Astonishingly, there were those that argued that this was not a security breach! Although it is true that, in general, photos of a vacationing family would not be considered sensitive, when you consider that the family taking the vacation includes the head of the British foreign intelligence service, it is easy to see how this kind of exposure could open the door to potential blackmail.We are all too aware of the possibility of terrorist "sleeper cells" living among typical American families under false identities. It is vital to understand how these individuals melt into the crowd, hiding their true identities while they hatch their nefarious plots. Recent events in Denver and New York City only serve to underscore the urgency of this need. This article will examine social networking in the context of social engineering. There are no easy or fast solutions to this problem, and this paper does not pretend to propose any. Rather, it is the purpose of this paper to enhance understanding of this very critical issue, and perhaps assist organizations and security professionals in developing policies and training which will mitigate this risk.

The Weakest Link: The Risks Associated with Social Networking Websites

By Yosef Lehrman[1]

Introduction

The relatively rapid rise in popularity of social networking services is now well known. MySpace, Twitter, and Facebook have become well known sites and terms. According to the Web traffic tracking site Alexa.com, as of December 2009, Facebook had 350 million registered users,[2] MySpace just under 475 million,[3] and Twitter 44.5 million.[4] Many people think very little of posting prodigious amounts of personal information on social networking sites, not realizing that this information puts them at risk. Specifically, those in the law enforcement and military communities may not realize that information posted on these sites can compromise operational security and potentially endanger lives. In July 2009, the Associated Press ran a story which was picked up by most major news outlets in the USA, in which it was reported that the wife of the incoming head of Britain's MI6 intelligence agency had posted pictures and family details on her Facebook page.[5] Astonishingly, there were those that argued that this was not a security breach! Although it is true that, in general, photos of a vacationing family would not be considered sensitive, when you consider that the family taking the vacation includes the head of the British foreign intelligence service, it is easy to see how this kind of exposure could open the door to potential blackmail.

We are all too aware of the possibility of terrorist "sleeper cells" living among typical American families under false identities. It is vital to understand how these individuals melt into the crowd, hiding their true identities while they hatch their nefarious plots. Recent events in Denver and New York City[6] only serve to underscore the urgency of this need. This article will examine social networking in the context of social engineering. There are no easy or fast solutions to this problem, and this paper does not pretend to propose any. Rather, it is the purpose of this paper to enhance understanding of this very critical issue, and perhaps assist organizations and security professionals in developing policies and training which will mitigate this risk.

The Weakest Link: The Human Factor

Imagine a security analyst, hired to probe an organization's security and determine potential entry points that can be exploited by an attacker. The company in question is so security conscious that it has spared no expense on both physical and cyber security systems. The company has extremely detailed and rigorous security policies and training, which are mandated for all employees. There are no passwords under keyboards or taped to the side of the computer monitors. Individuals walking the halls without proper identification displayed can expect to be stopped and questioned. Administrators are conscientious about making sure all security patches and antivirus updates are applied to their systems; it goes without saying that every system is equipped with antivirus and firewall software. Most people would be impressed with the level of security at this company. However, if the assessment was done correctly, it will show that this company is still highly vulnerable to a security breach.

How can a company such as this one be vulnerable? The answer is that unless the company has a clear plan and mandated training and retraining of all employees, a determined attacker can gain access to highly sensitive information by simply asking for it. According to testimony by security consultant (and reformed hacker) Kevin Mitnick before the U.S. Senate in March of 2000, he was routinely able to gain access to sensitive information just by asking for it.[7] Many companies cling to the illusion that their data is secure because of their investment in a cutting edge technological security solution, such as "biometrics,"[8] "two-factor authentication,"[9] or "smart cards."[10] However, treating security as a purely technological problem virtually guarantees that these organizations will suffer a security breach, as they have overlooked the weakest link in the chain of security—the human factor. Indeed, as the technological barriers to cracking a network's defenses are strengthened, it becomes more propitious for attackers to attempt to break into a network via the human element. This typically takes no more than a phone call or two, and involves minimal risk, while yielding a potentially substantial payoff.

Social Engineering and Abuse of Trust

To break the "weakest link" and defeat security measures by exploiting the human factor, an attacker must find a way to trick a trusted user into providing access or revealing information. This type of action is referred to as social engineering. Social engineering is defined as "the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking tech-

https://digitalcommons.usf.edu/jss/vol3/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.3.2.7

niques."[11] Social engineers (the term used to describe those who engage in social engineering) typically exhibit strong people skills; they are charming and likable. Particularly in Western societies, where people live their lives with the assumption that the majority of people are not trying to deceive them, and the overall probability of being misled is low, people tend to lose sight of this threat. A good social engineer will exploit this innate trust in other human beings, and make a request that sounds so reasonable that it raises no suspicion at all. However, it is possible that any information provided, no matter how innocuous it seems, can be that final piece of information needed to complete the attack.

There are many examples of attacks which were carried out with what appears to have been harmless information. In September 2008, it was reported that the personal email account of Sarah Palin had been accessed by an unauthorized user.[12] At the time, Palin was Governor of Alaska, as well as the Republican Vice Presidential nominee. Amazingly, the attacker accessed her email with astonishing ease. First, the alleged attacker acquired the username (which was easy to do, as that is typically the same as the first portion of her email address), and then misrepresented himself as her, by claiming to be the legitimate owner of the account and having forgetten the account password. The email provider then requested some personal information such as zip code, high school, etc. to reset the password. This information was easily obtained via Internet search engines. The actual attack took under one hour to pull off. Would people post the password to their email accounts online? Obviously not. However, many people see nothing wrong with posting tremendous amounts of personal information online, perhaps reasoning that little harm can result, since after all, it is only one single piece of information, which in and of itself is worthless. In truth though, the attacker uses these bits of information to compile a complete profile of the victim, which can then be used to mount a succesfull attack. Indeed, the May 2009 attack against Twitter.com utilized this method.[13]

Social Networks: A Potential Security Risk

While social networking services have become widely known and immensely popular, few realize the significant security risks that they present. Social networking services provide a large amount of personal information and raw data about people, organizations, and governments, which can be accessed relatively easy and anonymously. This information can then be used to target the victim. The United States military has recognized this as a concern, specifically as it relates to government employees and military service members. There have been articles in several Air

Force Base newspapers discussing the risk that social networking posts can pose to operational security. According to the results of a study of 500 U.S. Air Force members with MySpace profiles, over 300 individuals provided enough information on MySpace to make them vulnerable to a cyber-attack or blackmail—in military parlance "adversary targeting."[14] Fewer than 100 members were found to have low vulnerability (A graphical representation of the results of the study is provided in Figure 1). Vulnerability was established by how much information was provided, including name, hometown and state, duty location, job type, and whether the profile was public or private. In summary, the report found that over 60% of the members surveyed posted too much information.

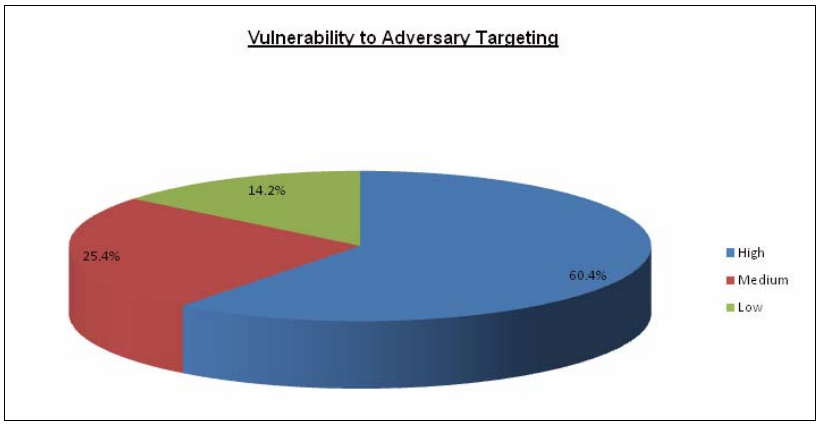

Figure 1: Percentages of USAF Personnel Posting on MySpace Vulnerable to Adversary Targeting

Social networking services have evolved dramatically from their inception in the late 1990s. What began as a venue for allowing people to meet and link with each other via email, has morphed into complex web-based sites, where people can maintain a "buddy list" of friends, chat with them in real time (instant messaging), and use a variety of applications built into the site to communicate. In so doing, these services have brought an inordinate amount of previously private information into the public domain. One mechanism by which social engineers can manipulate users of social networking sites is by actually becoming online "friends" with the target. Once the friendship is confirmed, the social engineer will then proceed to mine the victim for the information he or she is looking for; carefully planting key questions into an otherwise normal conversation. The myriad of risks that this issue can pose to military personnel was identi-

https://digitalcommons.usf.edu/jss/vol3/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.3.2.7

fied by the military over two years ago. To quote U.S. Air Force Staff Sgt. Joshua Liebold, "As far as people talking about themselves...a foreign spy information gatherer could look at [your information] and say, 'OK, that might be something to look into. Let's be their friend on MySpace.'...They mine you for information."[15] In fact, in August 2009, the U.S. Marine Corps issued a one-year ban on accessing social networking sites from its enterprise network, due to security concerns.[16]

Social Networking and Cyber Attacks

Another mechanism through which social engineers can leverage social networking services in a cyber attack is to gain the trust of the target by pretending to be a user who is trusted by the target. A classic example of this "abuse of trust" is the Koobface worm or virus. This worm (which has an ultimate goal of stealing personal financial information) spreads by delivering Facebook messages to people who are friends of a Facebook user whose computer has already been infected. The message directs the recipients to a third-party website, where they are prompted to download what is purported to be a legitimate file. However, if the file is downloaded and executed, it will infect their system as well.

A more recent example is the alleged attacks on Google and other corporate entities, which became public in mid-January 2010. Although the targets of these attacks were major commercial companies, they could just as easily have been military, law enforcement, or government. The malware was secreted in an encrypted image file hosted on a website maintained by the attackers. The target was directed to the malicious website through a carefully crafted "lure" email message. While it has not yet been proven, it is not unreasonable to assume that the attackers researched the target's personal preferences, hobbies, etc. using information that is publicly available through social networking services in order to aid in the crafting of the "lure" email, particularly given the pinpoint targeting of the target.

The purpose of this article is not to discuss the technical details of these attacks. Nevertheless, there is one aspect of these attacks that stands out as an emerging trend in cyber attacks in general. The success rate of the attacks is astounding. Virtually all users who received the malicious email were duped by the lure, and clicked on the link. Since it is obvious that the success rate of the attack is directly proportional to the thoroughness of its planning, it is quite clear that this attack was exceedingly well planned. A major part of that planning likely involved carefully scoping the targets—quite possibly using social networking sites.

Acquiring and Approaching the Target

One of the most critical components of a cyber attack through social networking sites is identifying a target. The attacker is typically looking for a user who will have access to high level or sensitive information. In order to help locate these users, the attacker may do some research using search engines such as Google. Most corporate entities make at least part of their corporate structure available on the public Internet. Military and law enforcement agencies may have notices of appointment and/or promotion carried by the local press. All of this information is cataloged by search engines and made generally available to anyone who looks.

Once a target is identified, the attacker cannot send a random email with a link to the malicious site or the malware itself. Most computer users know never to open attachments or click on links from unsolicited emails. Additionally, by sending a random email, the attacker decreases the chance of a successful attack. After all, the attacker must be reasonably certain that the target will open the document, or click on the link and thereby activate the payload. Trying to get someone who is afraid of heights to open a document ostensibly containing a quote for mountaineering paraphernalia simply will not work.

The attacker may then turn to social networking services, looking for any information that would make the target more easily compromised. Information of value could include upcoming events, travel plans, associates, likes and dislikes, etc.—in short, just about anything that the attacker can use to increase credibility. Supposing a scenario where the target does not directly post any information that can be of use to an attacker, or if such information is posted, it is not made available to those not on the target's "friend list," the target may still be vulnerable. A savvy attacker can attempt to become online "friends" with individuals on the target's "friend list." He or she could then reach out to these associates to discuss what appear to be topics of mutual interest, but in reality are attempts to learn about the industry. The target may have configured the security settings on the social networking service site to prohibit strangers from seeing the profile, but to allow "friends of friends" to see it. This provides the attacker with the information needed to construct a lure email message which is likely to deceive the target.

Security through Obscurity

It should be clear from the above that social networking services can pose a very real hazard to the security of corporate entities, government offi-

https://digitalcommons.usf.edu/jss/vol3/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.3.2.7

cials, and law enforcement personnel. In order to protect their privacy, and themselves, users should be encouraged to have as little personal information as possible publicly available. Specifically, while it has become popular for high-ranking government officials to reach out to their constituents via social networking services, the security risks must be borne in mind and addressed. Users should not make their profiles available to everyone, and should avoid accepting friend requests from unknown sources. Strangers online should be treated like strangers offline—maintaining requisite politeness and distance. Consider that unsolicited friend request as a request for personal information from a person who sat next to you on a bus. No rational person would hand over confidential information to a complete stranger.

Conclusion

Researchers have identified a paradox in the realm of security called the "Paradox of Usable Security," which states that "The more secure the technology, the less secure the system."[17] In other words, the technological complexity of the security of a system is directly related to users' attempts to circumvent it. This would seem to imply that having too much security could be less than beneficial when not coupled with sound personnel security and accountability programs. At the same time, a deficiency in security can leave an organization vulnerable to attack. The answer to this conundrum of course, is that security is a balancing act. The challenge is to find the proper balance of security and productivity.

It is an unfortunate but very real fact is that we do not live in a world where we can rely on all people to act in an honest and trustworthy manner all the time. As a society, we must constantly be vigilant, on the lookout for those who would attempt to deceive us, from within and outside. It is important to realize that anyone can make use of social networking sites and social engineering tactics to compromise operational and personal security. Taking some commonsense steps to protect personal information can go a long way in protecting ourselves and our organizations from those who seek to do us harm.

About the Author

Yosef Lehrman received his Masters of Science in Internet Technology/ Information Security from Pace University. He is also Microsoft-Certified (MCSA) and the holder of vendor neutral security certifications. Yosef currently works for the NYPD in the identity and access management areas. In addition to these technologies, he also supports Active Directory,

Active Directory Certificate Services (ADCS) and related technologies. He can be reached at *ylehrman@gmail.com* for questions or comments.

References

1 The opinions in this article are solely those of the author, and do not in any way reflect the opinions or policies of the New York City Police Department.

2 *http://www.alexa.com/siteinfo/facebook.com*

3 *http://www.alexa.com/siteinfo/myspace.com*

4 *http://www.alexa.com/siteinfo/twitter.com*

5 *http://www.foxnews.com/story/0,2933,530124,00.html*

6 In September 2009, Najibullah Zazi, a legal U.S. resident, was arrested and charged with conspiracy to use weapons of mass destruction. Zazi lived in Denver and in January 2009 made a trip to Pakistan where he allegedly received explosive and weapons training. Zazi was also allegedly plotting to detonate explosives in New York City, possibly intended to coincide with the anniversary of the 9/11 attacks. What makes this case particularly frightening is that according to government sources quoted in the Wall Street Journal, this is the second case of a U.S. resident receiving terrorist training overseas and then returning to plan an attack in the US since 9/11. Cam Simpson and Evan Perez, "U.S. al Qaeda Cell Suspected," *Wall Street Journal*, available at: *http://online.wsj.com/article/SB125374801698835711.html*.

7 Kevin Mitnick, Testimony before the U.S. Senate Governmental Affairs Committee, March 2, 2000, available at: *http://mitnicksecurity.com/media/SGAC-Testimony-20000302.pdf*.

8 A.K. Jain., A. Ross, S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology* 14, 1 (2004): 4–20.

9 Yang, Guomin, Duncan S. Wong, Huaxiong Wang, and Xiaotie Deng, "Formal Analysis and Systematic Construction of Two-factor Authentication Scheme," *Lecture Notes on Computer Science*, Vol. 4307 (2006): 82–91.

10 "About Smart Cards: Introduction: Primer," Smart Card Alliance, available at: *http://www.smartcardalliance.org/pages/smart-cards-intro-primer*.

11 Joan Goodchild, "Social Engineering: The Basics," *CSO Online*, available at: *http://www.csoonline.com/article/514063/Social_Engineering_The_Basics*.

12 Michelle Malkin Blog, available at: *http://tinyurl.com/2envcdy (michelle-malkin.com/2008/09/17/the-story-behind-the-palin-e-mail-hacking)*.

13 Robert McMillan, "Hacker: I Broke into Twitter," Network World, available at: *http://tinyurl.com/cdmzqc (www.networkworld.com/news/2009/043009-hacker-i-broke-into.html?nlhtsec=ts_050109&nladname=050109securityal)*.

14 Jeffery Carr, *Inside CyberWarfare* (Sebastopol: O'Reilly Media, Inc., 2009).

https://digitalcommons.usf.edu/jss/vol3/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.3.2.7

15 Quoted by: Travis Air Force Base News. MySpace, Facebook, more pose challenge, *United States Air Force*, available at: *http://www.travis.af.mil/news/story.asp?id=123101954*.

16 The text of the ban is available at: *http://www.marines.mil/news/messages/Pages/MARADMIN0458-09.aspx*.

17 Andrew Swartz, "Andrew's Usability in the Real World: The Paradox of Usable Security," *Usability News*, available at: *http://www.usabilitynews.com/news/article1875.asp*.

Journal of Strategic Security

https://digitalcommons.usf.edu/jss/vol3/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.3.2.7