ITM Whitepaper

ILLINOIS INSTITUTE OF TECHNOLOGY | *School of Applied Technology*

...because knowledge is power.

Effective Training and Policy Takes the Fear out of Social Networking

Shawn Davis
Edited by Ray Trygstad

11/25/10

www.itm.iit.edu

An Information Technology and Management Whitepaper from
Illinois Institute of Technology's School of Applied Technology

ITM Whitepaper: *Policy and Training for Social Networking*

The exponential growth of social networking websites over the last five years has created a new dimension to the lives of online users. It only takes a few minutes of viewing Facebook's news feed to witness the inherent excitement people display from sharing their thoughts, opinions, and information with a wide base of other users. This excitement has created a real problem for today's organizations that are not prepared to deal with the overall security implications that can arise from the use of social networking by employees in and away from the workplace. Organizations must realize they cannot simply purchase a technological solution and expect to be safe from attack. While technology based controls are helpful in dealing with these threats, the true weakest links are your end users. The creation of a clear policy in conjunction with a smart and engaging training process for end users is the single most effective way to eliminate much of this risk. Before one can begin to design an effective social media policy and training process, it is important to understand what social networking is.

What is Social Networking and why is it a danger?

Technical author Joey Bernal defines social networking as "the creation of a virtual community where users can share, discuss, collaborate, and even argue about topics of common interest".[1] Social networking is described by the CEO of the firm HGGary, Greg Hoglund, as a "digital version of a relationship"[2]. Both descriptions are spot on, but Hoglund's is especially accurate in describing the main reason that social networks are such a popular attack vector. People primarily use social networking, also known as social media, to build relationships and often feel quite comfortable disclosing details about their work and life with complete strangers. This is due to a perceived sense of security from being online. While a sensible person would usually not provide any personal information to a complete stranger on the street, this type of details are exactly what a large number of people provide to attackers online. There are several social networking sites out there today but attackers generally use the sites most popular with users.

As of October, 2010, the top four social networking sites in terms of estimated unique monthly visitors are: Facebook at 550 million visitors, Myspace at 90.5 million visitors, Twitter at 89.8 million visitors, and LinkedIn at 50 million visitors[3]. A survey sent out in 2009 asked over 500 organizations which social network posed the biggest risk to security in their opinion. Roughly 60% of respondents named Facebook as the biggest risk followed by Myspace at 18%, Twitter at 17%, and LinkedIn at 4%[4]. The survey also has shown that "over 72% of firms believe that employees' behavior on social networking sites could endanger their business's security"[5]. The monthly visitor counts and survey data both show a direct correlation of visitors to security risk among these four websites. The majority of the danger of social networking comes from too much available user profile information, social engineering attacks, and how quickly and widespread reputation damage can occur.

Attacks that exploit social networking

Social networking profiles often display a wide variety of information that is valuable to attackers. This information often referred to as Personally Identifiable Information, or PII. Too much PII can create a security concern for organizations due to the increased risks of aiding various attacks. This vulnerability is most prominent among Facebook, Myspace, and LinkedIn due to the ease that personal information can be made publically available. Information that can be publicly listed varies but can include a user's name, family member names, marital status, education and work history, a brief biography, religious and political views, birth date, phone numbers, IM screen name, current city and state, hometown, likes and interests, income level, ethnicity, and their email addresses.

---

1 P. 14, Bernal, J. (2010). *Web 2.0 and social networking for the enterprise: Guidelines and examples for implementation and management within your organization* [Electronic version]. Boston, MA: Pearson Education. 14.

2 Messmer, E. (2009). "How to handle social networking security risks." Retrieved October 8, 2010, from http://www.cio.com/article/490786/How_to_Handle_Social_Networking_Security_Risks?page=1&taxonomyId=3089

3 eBizMBA Inc. (2010). Top 15 most popular social networking websites. Retrieved October 13, 2010, from http://www.ebizmba.com/articles/social-networking-websites

4 Sophos. (2010). *Security threat report: 2010.* Retrieved October 8, 2010, from http://i.zdnet.com/blogs/sophos-security-threat-report-jan-2010-wpnaIbid.pdf?tag=mantle_skin;content

5 *Ibid.* 3.

For a user, all of this PII mainly presents the possibility of identity theft. In terms of risk to an organization, one way attackers often use this information is to acquire user logon credentials.

Attackers will use this information for password guessing and also for narrowing the parameters in password cracking attacks. They will also often circulate chain messages among users in the form of a survey or quiz. Brad Dinerman of GFI had received one of these survey messages that asked about his first elementary school, favorite pet's name, etc[6]. Brad made the connection that several of these questions are the exact same secret questions used as password reminder questions by banks, ecommerce sites, and Human Resources employee portals. Robert McMillan of IDG News writes about an example of a password reset attack:

> *A hacker going by the name of GMZ said he was able to gain access to an administrative account by guessing the password of a Twitter support staffer. The password was reportedly an easy-to-guess word: happiness. GMZ then used that access to take control of 33 high-profile accounts, including those for [Britney] Spears, U.S. President Barack Obama and Fox News.*[7]

Attackers also realize that users often create passwords based on information in their profiles such as a child's or spouse's name and birth date. Aside from password acquisition, too much PII can also aid in another common type of attack that requires a little more creativity from an attacker.

Social engineering attacks are widely used across all four of the main social networking sites. This threat occurs when an attacker uses social skills to trick a user into revealing their password or other private information. Attackers will often target specific users through searching social networking sites for specific companies, groups, or organizations. Information will then be gathered on the target from the sites to be used as an attack vector against them as described by the Federal Bureau of Investigation in a 2009 Headline Alert[8]. The attacker will study PII, message posts, and friend lists in order to learn more about their target and develop a trust relationship. Once trust is built, the attacker may try to compromise the security of the target's company network or gain confidential insider information. The attacker will also try to use this relationship to gain the trust of other employees to further penetrate the organization[9]. It has been documented that many cyber criminals would rather engineer a user to uncover information than use their efforts to attack the technology and controls for security. This is due to the rush of the con and the high success rate of engineering today's disenfranchised workers[10]. This shows that an organization can't afford to put all of their resources into technological controls. It is absolutely vital to the security of the organization that end users receive training on these threats. The fact that this training is often missing only encourages more attacks. These attacks do take a decent amount of time though which leads us to a more efficient form of social engineering called phishing.

Phishing, also known as spear phishing, targets "a specific user or group of users, and attempts to deceive the user into performing an action that launches an attack"[11]. The breakdown on how these attempts are distributed include: 52% by a user opening an attachment, 16% by a user clicking a link, 9% by link redirect, and 3% unknown[12]. These attacks frequently are delivered through social networking sites or email and use personal user information to make these messages more believable. A common example is an email that that pretends to come from LinkedIn inviting the user to connect on Twitter. The email may ask the user to open an attached zip file that contains a mass mailing worm or click a link that is connected to a spam site in order to view the invitation[13].

6 Dinerman, B. (2010). *Social networking and security risks.* Retrieved October 13, 2010, from http://www.gfi.com/whitepapers/Social_Networking_and_Security_Risks.pdf

7 McMillan, R. (2009). "Hacker: I broke into twitter." Retrieved October 8, 2010 from http://www.pcworld.com/businesscenter/article/164182/hacker_i_broke_into_twitter.html?tk=rel_news

8 Federal CIO Council (FCIOC) (2009) *Guidelines for secure use of social media by federal departments and agencies.* Retrieved October 8, 2010, from http://cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf

9 *Ibid.*

10 Tipton, H. F., & Krause, M. (2007). *Information security management handbook* [Electronic version]. (Sixth edition.) Boca Raton, FL: Auerbach Publications.

11 FCOIC. 9.

12 Graham, J. (2009). *Cyber fraud: Tactics, techniques, and procedures* [Electronic version]. Boca Raton, FL: Auerbach Publications.

13 Dinerman.

Another common ruse involves hiding a malicious website link in a shortened URL with a service provided by sites such as http://tinyurl.com/ and http://bit.ly/. The attacker will often send these shortened links in a devious private message or as a post to a user's wall for all of their connections to see and possibly click on[14]. Phishers regularly also use automated malware distribution schemes to increase their efficiency.

A common means of distribution comes from using Cross Site Scripting (XSS). XSS is a common attack vector in social networking that allows an attacker to inject malicious scripting into a web page. A 2006 XSS attack compromised close to 34,000 usernames and passwords from Myspace[15]. Another method for password acquisition involves a user clicking on a malicious link that installs a keylogger that transmits user authentication data back to the attacker[16]. Passwords for social networks are highly sought by Phishers due to fact that the attacker can then send messages to a user's contacts. The user's contacts are much more likely to open a message from a trusted contact and activate the malware. This is why it is imperative that users not use the same password for all of their sites.

One of the more famous distributions is the Koobface worm. Internet security firm Sophos (2010) maintains that:

> *The sophistication of Koobface is such that it is capable of registering a Facebook account, activating the account by confirming an email sent to a Gmail address, befriending random strangers on the site, joining random Facebook groups, and posting messages on the walls of Facebook friends (often claiming to link to sexy videos laced with malware). Furthermore, it includes code to avoid drawing attention to itself by restricting how many new Facebook friends it makes each day.*[17]

Another popular malware distribution method can arise from a user allowing the various add-on entertainment applications that are circulating in Facebook to have access to their account. An example is the "Secret Crush" application which installs a java based keylogger onto the user's system through the Zango malware program[18]. All of the threats thus far have been based on what an attacker can do. The last main threat is created by users themselves and can damage their own reputation as well as that of their organization.

Potential impact on enterprise reputation

As previously mentioned, all four of the main social networking sites allow information to be posted publicly. Users often fall into the habit of using their social networking profiles to provide a live play-by-play of their life. They just do not think about the fact that information on the internet travels very quickly and stays around a long time. Hypothetically, imagine an employee named Jim who works in the development lab of Fortune 500 company XYZ Corporation's smart phone division. Jim gets home from work one day and logs into his Facebook account. He has mostly childhood and college acquaintances in his friend list but also happens to have added a few fellow developers he had met at an industry conference last year. After a long and frustrating work day, Jim decides to vent to his Facebook friends to ease his stress. He posts: "Nothing seems to be going right today at work. At this rate the huge project I am working on will not come together before Christmas and may not at all. I need a drink…" Kristen, one of the developers from the industry conference, notices this message and remembers that Jim is XYZ Corporation's top smart phone developer. Kristen quickly passes a screenshot of this post on to the distribution manager of her company which is XYZ Corporation's biggest rival. This particular manager had been trying to get their next smart phone picked up by the largest carrier network for the holiday season. The carrier liked both phones but could only pick one of the two and was mainly concerned about the Christmas deadline that both

14 *Ibid.*
15 FCOIC.
16 IT Governance Research Team (2009). *How to use web 2.0 and social networking sites securely – a pocket guide* [Electronic version]. Cambridgeshire, UK: IT Governance Publishing
17 Sophos. (2010). *Security threat report: 2010.* Retrieved October 8, 2010, from http://i.zdnet.com/blogs/sophos-security-threat-report-jan-2010-wpna.pdf?tag=mantle_skin;content
18 FCOIC.

had promised to. The rival manager quickly set up a meeting with the carrier's buyer and showed their current progress and also a screen shot of Jim's post about XYZ Corp. not being able to hit the deadline. That settled things for the buyer and XYZ Corporation ended up losing a multi-million dollar deal. Now this was just a fictitious story, but situations like this one can and do occur.[19]

Gartner Inc. analyst John Pescatore mentions an example where an employee of a campground chain decided to be helpful and post a spreadsheet on Facebook showing the reservation status of their different camp sites. Unfortunately, this spreadsheet also included the credit card numbers of the campers that had reserved the sites[20]. In another example, Jeff Hayzlett, the former chief marketing officer at Eastman Kodak Company admits to posting a potentially damaging tweet on Twitter about one of their products. Jeff states that, "I accidentally hit send instead of save and tweeted out what we had worked six months to protect"[21]. While the above examples definitely cause reputation damage, an even more damaging post happened to a major fried chicken chain in 2008. A worker there posted on their profile, "I just posted a funny video of myself frying a rodent at the restaurant where I work"[22]. It is definitely easy to see the many consequences that could occur from a video like that hitting the news outlets. A clear social media policy and specific end user training that covers guidelines for posting will not only save many organizations from these costly accidents but also cut down the risks of costly litigation.

Necessity for Social Media Policy

An employee that is fired for making negative twitter posts could take legal recourse against their employer if they can prove that due care was not being demonstrated. The employee would simply have to show that a policy was either not in place or that they were unaware of it. They may also be able to prove that other employees or members of management had made the same types of posts without consequence. An organization is legally responsible to exercise due care and due diligence in regards to social networking use by its employees. An organization cannot demonstrate due care if it refuses to take measures to ensure that every employee is aware of what is and is not acceptable in the workplace as well as the consequences of actions that are illegal or unethical [23]. An organization must demonstrate due diligence by ensuring that it is making a continuing effort to protect others. The far reach of the Internet makes it possible for an organization to wrong a person in practically any country or state. This creates an even greater chance for potential litigation[24]. It would seem crazy that any organization would not take a few simple steps to protect themselves. Surprisingly, this failure seems to happen all too often.

In 2007, *Computerworld* asked its readers if they had a policy in place regarding social networking use at work. The responses show 41% did not, 52% did, and 7% didn't know[25]. Of those surveyed, 20% stated that they planned to work on putting together a social media policy within the year. In September of 2009, *Computerworld* executed a similar follow-up survey and the results were 41% did not, 53% did, and 6% did not know[26]. It appears that only the 1% that didn't know in 2007 must have figured out that they actually did have a policy in place. The 41% of organizations without a policy did not change. *Computerworld* also references the following two examples:

> *In a July 2009 poll by advertising agency Russell Herder and law firm Ethos Business Law, both based in Minneapolis, 81% of the 438 respondents said they have concerns about social media and its implications for both corporate security and reputation management. However, only one in three said that they have implemented social media guidelines, and only 10% said that they have undertaken related employee training.*

19 Brandel, M. (2009). "Baited and duped on facebook." *Computerworld*, 43(31), 28-33.
20 Mitchell, R. L., (2009). "Scams, spams & shams: Online social networks put a new face on brand damaging activities, ranging from reputation attacks to imposter sites." *Computerworld*, 43(31) 23-25.
21 *Ibid.*
22 Dinerman. 9.
23 Whitman, M. E., & Mattord, H. J. (2010). *Management of information security*. Boston, MA: Course Technology.
24 *Ibid.*
25 Brandel.
26 *Ibid.*

> *A Deloitte LLP survey echoes those results. Only 15% of 500 executives polled said that the risks of social media are being addressed in the boardroom, although 58% said they agree that it's important to do so. But even those that do have policies may not effectively communicate them. Of 2,008 employees that Deloitte surveyed, 26% said their employers had guidelines regarding what they could say online, 24% said they didn't know if their employers had such a policy, and 11% said that there was a policy but they didn't know what it was.*[27]

With all of this potential for litigation as well as the many other threats, why are organizations not taking the time to develop an effective social media policy and train their end users properly? The answer starts with the culture of the organization.

There are some organizations that do not put much thought or resources into information security period, and probably don't recognize the need for a social media policy. This often comes from a lack of engagement in upper management. It is vital for the information security function to have C-level support financially and administratively[28]. Other organizations may feel that their best choice is to just block all social networking sites from their network and not worry about policy or training. This approach actually puts an organization into even greater danger for several reasons. One reason is that users will find a way around the block and still gain access, allowing all threats to occur. Secondly, users could still access these sites at work with mobile devices or just wait until they get home. Even though mobile device or home use might free up some network bandwidth and decrease malware, all other threats could still occur. Thirdly, without a policy and training in place, these organizations are wide open for litigation. Lastly, blocking these sites will take away all of the great benefits that come from social networking. These benefits include: increased collaboration, a more interactive relationship with customers, increased vertical networking among colleagues, sales and marketing strategies, and incentivized working conditions for younger members of the workplace[29]. Now that the need for a policy and training has been established, where does one begin?

Creating an enterprise Social Media Policy

Tiffany Black, a social media trainer for mediabistro, recommends that a policy focus should "be more about what employees can do and best practices for social media use versus all the things employees can't or shouldn't do on social media"[30]. A social media policy is really just an extension of an organization's acceptable use and other existing policies. The creation of this document should be a joint effort by information security, information technology, human resources, legal, and end users. This group should be led by a team leader often employed in an information security or risk management function. As previously mentioned, it is also imperative to have a project champion with the ear of upper management to ensure financial and administrative support[31]. A good first step in creating a social media policy is to review policies of other organizations. A great online resource for this is the Social Media Governance database at http://socialmediagovernance.com/policies.php. Their site has many social media policies from various organizations for review. While these policies may share some similarities, it is very likely that each organization will have very different philosophies on social media use. A liberal arts college, a global corporation, and a government agency, for example, would probably not all be able to use the same social media policy.

The liberal arts college may encourage unrestricted information sharing and allow open access to all social networking. Their policy will still need to cover all potential threats but may focus mainly on guidelines for posting. The University of Michigan's social media policy starts off with general rules to follow and then has separate guidelines for posting as an individual versus posting on behalf of the University. They end with a section on safety and privacy tips for social networking that cover such topics as privacy, personally identifiable information, liabilities, and malware[32].

27 *Ibid.*
28 Whitman and Mattord.
29 IT Governance Research Team (2009). *Threat 2.0: Security and compliance for web 2.0 sites* [Electronic version]. Cambridgeshire, UK: IT Governance Publishing.
30 Black, T. (2010). *How to write a social media policy.* Retrieved November 5, 2010, from http://www.inc.com/guides/2010/05/writing-a-social-media-policy.html
31 Whitman and Mattord.
32 University of Michigan (2010). *Guidelines for the use of social media.* Retrieved October 8, 2010, from http://www.voices.umich.edu/docs/Social-Media-Guidelines.pdf

The global corporation will often use social media for brand management as well as a sales and marketing tool. Their policy will need to cover most all possible threats and may focus on reputation damage and data leaks. The Coca-Cola Company's social media policy starts with their company vision and commitments and then delves into principals and expectations. Similar to the University of Michigan, Coca-Cola also has different guidelines for individual use versus company business use. Coca-Cola then uses a great method for taking this a step further by designating and requiring training for specific certified online spokespeople. These certified spokespeople are the only employees allowed to speak on behalf of Coca-Cola online[33].

Government agencies will often have the strictest requirements in regards to social media use. In 2009 the Federal CIO Council in conjunction with its underlying committees and groups created a document entitled *Guidelines for Secure Use of Social Media by Federal Departments and Agencies*. The council states that "The decision to embrace social media technology is a risk-based decision, not a technology-based decision"[34]. The document has sections on risk, social media traits, threats, and recommendations for controls. These guidelines are intended to assist an agency in making a business case for social media use based on a risk management approach. The document specifically mentions spear phishing, social engineering, and web application attacks as the main risks[35].

After reviewing various policies it is helpful for the policy writer to choose a few that are similar to their organization's mission as a reference point. The next step is to evaluate your own organization's social networking use. It is recommended to involve end users to assist in this process. Also, find out what current and future plans sales, marketing, and any other department may have for using social media. After that, the information security function should analyze what threats the organization is most likely to face based on the organizational use as well as the personal use of end users at work and at home. Once that is complete, start the creation process and involve human resources. It is important to refer the end user to review their employment agreement and their employee handbook early on in the new policy[36]. Often, the employee handbook and/or acceptable use policy will need to be updated to list the consequences of not abiding by the guidelines of the new social media policy. The guidelines in the new policy should be drafted based on all of the information and feedback acquired from end users, information security, and human resources. It should also be noted that issue specific policies in regards to controls for bandwidth, malware, and content filtering may need to be rewritten to account for social media use. Once all of the sections and guidelines of the new social media policy are complete, the legal department will need to review the final draft of the new policy and any changes to other existing policies. This is to ensure all potential liabilities are covered that the organization could face. Once a final draft is approved by all parties involved, it should be submitted for approval by upper management. When final approval is granted the new social media policy will need to be distributed to all employees.

Distribution can either be in paper form or electronically, but in either case it's necessary to document that the user has agreed to the terms and conditions with a signature and date. This is to protect an organization from a user stating that they were not aware of the policy. The fact that the Deloitte LLP survey referenced earlier stated that 24% of the surveyed employees didn't know if their employer had a social media policy and 11% said there was a policy but were not aware of what it covered is a clear indication that this compliance step is often missed[37]. Once all users have signed and dated the policy, training needs to commence. The training program should be designed during the policy creation process and be ready for a rollout so there is no delay. Comprehensive training will not only protect the organization against threats but again also from liability. It is very difficult for an employee to state in court that they were unaware of a social media policy when it can be documented that they have completed a training course in addition to signing the compliance section of a policy.

33 Coca-Cola Company, (2010). *Online social media principles.* Retrieved November 5, 2010, from http://www.thecoca-colacompany.com/socialmedia/
34 FCOIC. 6.
35 *Ibid.*
36 Black.
37 Brandel.

Training in using Social Networking safely and sanely

A training course on social networking needs to be interesting and engaging, and should not be presented as a monotone PowerPoint session. Every employee from the CEO down should be required to attend this training to ensure compliance and to reflect a company-wide effort. There obviously will be things that end users can't and shouldn't do, but the training should be presented in the can-do manner as described by Black[38] to increase the likelihood of end user buy-in to the program. Some organizations will build-in training on social media marketing, but for the purpose of our discussion the training described will be limited to preventing information security threats and liability. Topics covered here are geared towards end user training and will include best practices in regards to personally identifiable information (PII), social engineering/phishing, and reputation damage. An interactive and experienced trainer should lead the session and have access to a live internet connection.

As participants are arriving, there should be a live social networking profile of a fictional employee showing on an overhead. The trainer should enter and ask the class what they think about this profile. After fielding a few answers, the trainer could ask what about this profile could be damaging if viewed by an attacker, a competitor, the media, investors, or the general public. This should start an open and interactive session and may very well be the first time that these users have taken a moment to really think about the possible damage that can occur from a seemingly reasonable social networking profile. This profile should have examples of the various threats that are presented from improper social networking use. An example profile of Jim Jones, the fictional smart phone designer at XYZ Corporation is shown on the following page in Figure 1.

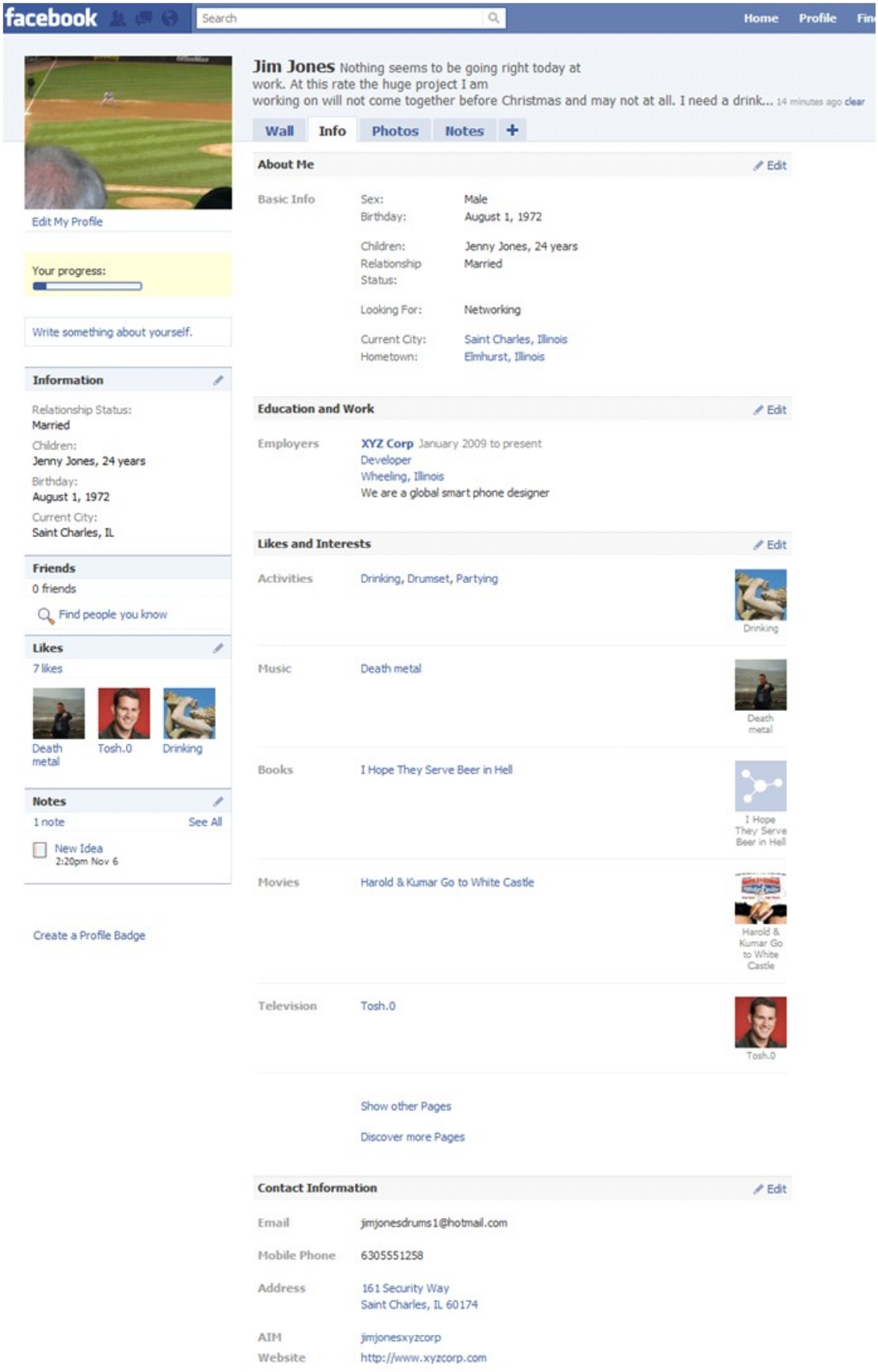
Jim's profile, while seemingly harmless, presents a lot of information to attackers. As previously discussed, too much PII in end user social networking profiles can lead to risks of password acquisition and aiding in other attacks. When creating the fictional employee's social networking profile, the trainer should also create a web based email account as well. In the example of Jim, the trainer will show the class that a Hotmail address is listed for him. The trainer will then open up a browser and go to Hotmail and type in Jim's email address as an attacker. Next, the 'Forgot your password?' link should be clicked and the reset password by security question option chosen. The security question in this example asks what his mother's birthplace is. The trainer then pulls back up the Facebook page and asks the class what would be a good guess for the mother's birthplace based on Jim's page. A member of the class might notice that Jim's hometown is Elmhurst and remark that would be a good first guess. Voilà!

The trainer now has access to Jim's Hotmail account and shows the class that Jim has been emailing confidential company schematics to himself so that he can work on them at home to avoid his company's secure but slower VPN. From here the trainer playing the role of the attacker is able to open several emails that show logons and passwords to various credit card and bank sites. One of these ends up being the same logon that Jim uses to access XYZ Corporation's corporate network. The more realistic the trainer can make the demonstration by creating the Hotmail and Facebook accounts for their own fictional employee and then using real emails and logons as examples on an active internet connection the better. These live demonstrations will really hit home for users that had read the policy but didn't actually think they were in danger. The trainer should then visit the privacy settings pages for the social networking sites most used by the organization's users and give a brief explanation. Lastly, the policy guidelines should be reviewed with the class to teach them what can and should be posted as well as what is against policy and dangerous to online safety.

This is also a good time to revisit strong password creation. The trainer should start with demonstrating that a good password consists of at least nine characters including upper and lower case letters, numbers, and symbols. It should also be completely random and not include any words or names. A modern 3.0 GHz Intel Core 2 based system is able to execute roughly twenty-seven million guesses per second (Whitman & Mattord, 2010). The trainer could explain this and take the class to a password calculator site such as http://lastbit.com/pswcalc.asp. It should be explained that this site calculates a brute-force attack which is used to crack a completely random password.

38 Black.

Figure 1. *Jim Jones' Facebook Profile*



The trainer can then manipulate the entry data to show how a strong password is useful. Table 1 below shows some various calculations from the LastBite site. For example, an attacker could crack a weak four character lowercase password with a modern system in about a minute with one computer. Increase that lowercase password to eight characters and it would take 90 days to crack. A strong password of eight characters using upper and lower case letters, digits, and punctuation would take an attacker with the same system 1,071 years to crack. By adding one more character to get nine characters, the time to crack is upped to 79,233 years. For this reason, nine characters are recommended over eight due to the exponential increase in time.

Table 1.
Brute-Force Password Cracking Table (based on results from http://lastbit.com/pswcalc.asp)

Password length	4	8	8	8	8	9	8
*Speed**	27	27	27	27	27	27	27
Number of computers	1	1	1	1	1	1	1000
Chars in lower case	X	X	X	X	X	X	X
Chars in upper case			X	X	X	X	
Digits				X	X	X	
Common punctuation					X	X	
Calculation (up to)	1 min	90 days	64 yrs	260 yrs	1071 yrs	79,233 yrs	129 mins

*Speed is depicted in the number of password guesses a processor can achieve in millions per second. (A 3.0GHz Intel Core 2 system can typically achieve 27 million guesses per second.)

One of the members of the class might remark that even an eight character password with only lowercase letters seems pretty secure based on the fact it would take 90 days for an attacker to crack. It should be explained that attackers also use dictionary attacks and that if this eight character password included any common words or names that it could be cracked much quicker. This will reinforce the reason that common words should never be included in passwords. It should also be explained that even if the password was completely random that attackers sometimes use botnets to increase their efficiency. Botnets are large groups of computers that an attacker can remotely control through malware and run distributed password cracking attacks from. For example, a 1,000 computer botnet could crack an eight character all lowercase random password in up to 129 minutes versus the 90 days it would take one computer. The trainer can then reinforce the argument for a strong password as well as the need to be vigilant against contracting malware.

While it is helpful to show examples of how long it can take a computer to break a password, it is also beneficial to actually demonstrate this. The trainer should be trained on how to use a basic password cracking program to perform a dictionary attack as well as a brute-force attack on hashes. Then the trainer could ask for a volunteer to type in a single word case-insensitive password that is four characters long as a user account password for windows. The trainer will then run a dictionary crack and show how the password was uncovered in seconds. The demonstration could go into a few other passwords that are longer, case-sensitive, and have characters to show how the strongest passwords could take years to crack.

The trainer should wrap up this section by revisiting the fact that Jim used the same passwords for multiple sites. Most users have many different online accounts that require credentials. Explain that users should never use the same password for each site even if it is strong. While it may be unlikely that this strong password will be cracked, even one single weak security question could allow an attacker entrance to an account. If the said account is for email, there will probably be user names and passwords to other sites. The trainer should recommend that if participants currently have weak passwords, the same password for each site, or weak reset questions, that they should fix these vulnerabilities for all online accounts as soon as possible. Also, remind users that they should never share their password and that no one at the organization should ever ask for it, including the information technology department.

The fact that Jim's profile is viewable by all presents him as an easy target for social engineers and phishers. His email, cell number, home address, company, work IM, as well as enough details of his life and family are listed for an attacker to start a conversation. Most users will even have much more information in their profile than Jim's. The trainer should pull up the profile and ask the class which pieces of information will give an attacker insight on Jim's life. Show how easy it is for an attacker to send what appears to be a legitimate message based on a small amount of information they were able to gather from Jim's profile. Then various examples of phishing emails and social engineering call texts should be shown to the class. In particular, show examples of the chain surveys that circulate these sites and how they are similar to password reset questions. Also, stress that even after a user uses the privacy controls that were just taught, that this privacy can be instantly erased by "friending" one person that is not known to them.

Next, examples of the various malware circulating schemes should be revealed to the class. Users should learn about never clicking on a link or opening an attachment if they are unsure of the sender. They should also be aware that often a phishing message can come from a compromised known sender. Traits such as misspellings, dialog that seems uncommon, and urgent messages should all be deemed suspicious. The trainer should also demonstrate that malicious links can be hidden in shortened URLs as well as make clear that pop ups should always be closed with alt-f4 or by using the task manager to prevent executing malicious code hidden in the exit button.

Reputation damage should be the last section of the training and have the most dialog around it. The trainer could start by again pulling up their fictional employee's profile page and asking what the class thinks about the person's status. In the case of Jim, this should start an interactive conversation about ramifications his status could have if viewed by competitors, the media, investors, and the public about XYZ Corporations smart phone business. The trainer can then discuss the guidelines as to whether the organization allows users to comment on behalf of the company. The Coca-Cola method of only allowing posts about the company to be made by certified online spokespeople appears to be a great method to lessen the risk of reputation damage. If this method seems appealing, a separate class should be devoted to certifying these individuals and then users in the main classes must be made aware of the restriction of posting about the organization within social media. Regardless, users should be taught best practices for posting messages to lessen their own risk of reputation damage.

The trainer should start conversation on various current examples that are in the news at the time of people and organizations damaged by postings. Stress to the participants that if they even have the slightest feeling that a post might be inappropriate, it is better to stop and give it some thought rather than just posting whatever comes to mind. It only takes one post to damage the reputation of a user or their organization and once posted there is often no going back due to the speed of information travel and the various Internet archiving sites that will store information for many years. Lastly, let users know that the organization cares about their online safety and wants them to be able to enjoy social networking. Ensure them that if they are ever unsure about a link, email, posting, etc. that they should consult with the organization's designated social media contact for guidance.

Once the training is complete, the trainer should have two completion certificates for each of the participants to sign and date. The trainer should then also sign and date the copies as well. One copy can be taken by the participants and the other should be stored in human resources personnel files. Again, this is to document that the user has not only agreed to and signed the social media policy but also to prove that the user has completed the training to protect the organization from being accused of not exercising due care. Remember that just because documents are signed and the training is over that the organization must not put social media out of sight or out of mind. Ongoing training and awareness is required to continue to demonstrate due care and to keep users fresh minded about protecting themselves as well as the organization against the various threats they have learned about. Finally, these policies must be enforced company wide. The quickest way to allow a social media program to become ineffective is by allowing certain users or management to be above the rules. Not only will this essentially make any policy void legally, it will also destroy all user buy-in previously gained.

In Conclusion...

While it will take some effort and elbow grease to design an effective social media policy and training program, the return on investment will be huge. Many threats from social networking are similar to existing pain points that information security professionals are already ailing over. Wouldn't it be great if every user in your organization finally saw the value of strong passwords and didn't mind the fact that their password changes every 60 days? What about if the level of malware infections on client systems and servers decreased 70% by having users truly understand which email attachments should not be opened? If this seems like an information security utopia, it won't really be. But it could be a great opportunity to finally start creating that security culture that is so highly coveted but previously seemed unreachable. If done correctly, this whole process can really bring an organization together and create a culture that is knowledgeable about information security and aligned in keeping their organization as well as themselves safe from harm.

ABOUT THE AUTHORS

Shawn Davis is a graduate student in the Information Technology and Management degree program at Illinois Institute of Technology. Shawn has worked in various roles in academic and corporate technology consulting since 2006.

Ray Trygstad is the Director of Information Technology for Illinois Institute of Technology's School of Applied Technology and the Associate Director of IIT's Degree Programs in Information Technology and Management. He teaches courses in open-source operating systems; operating system virtualization; multimedia; management for technical professionals; information systems security management; and incident response, disaster recover and business continuity. He also teaches in the Master of Public Administration program at IIT's Stuart School of Business.

References:

Bernal, J. (2010). *Web 2.0 and social networking for the enterprise: Guidelines and examples for implementation and management within your organization* [Electronic version]. Boston, MA: Pearson Education.

Black, T. (2010). *How to write a social media policy*. Retrieved November 5, 2010, from http://www.inc.com/guides/2010/05/writing-a-social-media-policy.html

Brandel, M. (2009). "Baited and duped on facebook." *Computerworld*, 43(31), 28-33.

Brandel, M. (2007). "Keeping secrets in a wikiblogtubespace world." *Computerworld*, 41(12), 26-30.

Coca-Cola Company, (2010). *Online social media principles*. Retrieved November 5, 2010, from http://www.thecoca-colacompany.com/socialmedia/

Dinerman, B. (2010). *Social networking and security risks*. Retrieved October 13, 2010, from http://www.gfi.com/whitepapers/Social_Networking_and_Security_Risks.pdf

eBizMBA Inc. (2010). *Top 15 most popular social networking websites*. Retrieved October 13, 2010, from http://www.ebizmba.com/articles/social-networking-websites

Federal CIO Council (2009) *Guidelines for secure use of social media by federal departments and agencies*. Retrieved October 8, 2010, from http://cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf

Graham, J. (2009). *Cyber fraud: Tactics, techniques, and procedures* [Electronic version]. Boca Raton, FL: Auerbach Publications.

IT Governance Research Team (2009a). *How to use web 2.0 and social networking sites securely – a pocket guide* [Electronic version]. Cambridgeshire, UK: IT Governance Publishing

IT Governance Research Team (2009b). *Threat 2.0: Security and compliance for web 2.0 sites* [Electronic version]. Cambridgeshire, UK: IT Governance Publishing.

IT Governance Research Team (2008). *Web 2.0: Trends, benefits and risks* [Electronic version]. Cambridgeshire, UK: IT Governance Publishing.

McMillan, R. (2009). "Hacker: I broke into twitter." Retrieved October 8, 2010 from http://www.pcworld.com/businesscenter/article/164182/hacker_i_broke_into_twitter.html?tk=rel_news

Messmer, E. (2009). "How to handle social networking security risks." Retrieved October 8, 2010, from http://www.cio.com/article/490786/How_to_Handle_Social_Networking_Security_Risks?page=1&taxonomyId=3089

Mitchell, R. L., (2009). "Scams, spams & shams: Online social networks put a new face on brand damaging activities, ranging from reputation attacks to imposter sites." *Computerworld*, 43(31) 23-25.

Sophos. (2010). *Security threat report: 2010*. Retrieved October 8, 2010, from http://i.zdnet.com/blogs/sophos-security-threat-report-jan-2010-wpna.pdf?tag=mantle_skin;content

Tipton, H. F., & Krause, M. (2007). *Information security management handbook* [Electronic version]. (Sixth edition.) Boca Raton, FL: Auerbach Publications.

University of Michigan (2010). *Guidelines for the use of social media*. Retrieved October 8, 2010, from http://www.voices.umich.edu/docs/Social-Media-Guidelines.pdf

Whitman, M. E., & Mattord, H. J. (2010). *Management of information security*. Boston, MA: Course Technology.

ITM Whitepaper: *Policy and Training for Social Networking*

ABOUT ILLINOIS INSTITUTE OF TECHNOLOGY'S SCHOOL OF APPLIED TECHNOLOGY

Illinois Institute of Technology's School of Applied Technology offers hands-on, project-based technology-oriented education and training for both full-time students and working professionals. Courses are taught by IIT professors and industry professionals with significant working, teaching and research experience in their fields. The School of Applied Technology offers degree, non-degree, certificate, credit, non-credit programs, corporate training, short courses and seminars ranging from a few hours to several days in length. Both Bachelors and Masters Degrees are offered in Information Technology & Management and Industrial Technology & Management, as well as Undergraduate Certificates in Industrial Technology & Management, Graduate Certificates in Information Technology & Management topics and adult education/CEU courses in all fields. Our Information Technology & Management curriculum is supported by extensive dedicated laboratory facilities. We offer an comprehensive range of courses in information security and business continuity.

For more information on our education and training programs in information technology, please see http://www.iit.edu/at/

Illinois Institute of Technology (IIT) is a private, Ph.D. granting university founded in Chicago in 1890, offering programs in engineering, science, technology, architecture, design, psychology, public administration, technical communication, business and law.