Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 3 (2015) 1096 – 1100

Procedia MANUFACTURING

6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE 2015

The human factor in the social media security –combining education and technology to reduce social engineering risks and damages

David Tayouri*

Israel Aerospace Industries (IAI), Israel

Abstract

Humansare social creatures and the digital era didn't change this, but it did change the way we communicate. Using social media we have instant access to millions of peoples and we have new ways of interaction. But the social media has security risks. It is used also by criminals for fraud, gathering business intelligence, stealing sensitive information etc. This paper will demonstrate the cyber security risks and mitigations, focusing on the human factor and social media. Formal policy to guide how employees can use social media sites is not enough, and complementary layers are needed: education starting at elementary school, interactive and adaptable training and innovative technology means. To strengthen the human factor, we should put effort in education, starting as early as the first grade, at the age that the children are exposed to the internet. Unusual approaches to cyber security training should be considered, such as interactive video games. But we should also put more effort on technological means of helping humans make fewer errors and avoid falling into cyber traps. Privacy settings can limit access to the user's information. Social media site monitoring tools can help organizations keep track of malicious activities and threats against them.Technology can help to check the reliability of the person suggesting friendship.Social networks can also be used to identify an organization's insider threat, by analyzing the social media content.Combining education and training with best-of-breed technology may reduce social engineering risks and damages.

Peer-review under responsibility of AHFE Conference

*Keywords:*Social media; Social engineering; Cyber security; Human factors

* Corresponding author. Tel.: +972-52-7201492; fax: +972-8-8575989.
*E-mail address:*dtayouri@elta.co.il

Peer-review under responsibility of AHFE Conference
doi:10.1016/j.promfg.2015.07.181

1. Introduction

Humans are social creatures – relationships and conversations between people are part of human nature. People always lived in groups and used to communicate around the fire, in city markets, in pubs or in café shops. The digital era didn't change this, but did change the way we communicate. Today we have many ways of digital communication. We can use Facebook to keep in touch with our friends and family, and to share with them posts, pictures and links. We have Twitter for micro-blogging, WhatsApp for instant messaging, Instagram to share pictures and YouTube for videos. LinkedIn is used for business social networking. There are many other sites, some for specific needs, some for specific groups.

Using social media we have instant access to millions of peoples and we have new ways of interaction. Wecan share our experiences with each other, be updated with our friends' statuses, support them when they need it, and read their statements. Within social networks we can read about people's recommendation on a product we want to buy or on a hotel in which we indent to spend our next holiday. People use social media for different reasons. According to the study "Why People Use Social Media Sites" (2009), 31% of social media users said that they want to get in contact with new people, 21% said that they want to keep in touch with their friends, and 14% mentioned general socializing as their reason[1].

People are becoming more comfortable using the Internet [2]. One common problem on social media web sites is over-sharing whereby people disclose too much information which in the long run might have unintended consequences. With social media people are now sharing information about their exact location, but sharing location-based information just means there is another layer of personal information exposed which may not always be really necessary. If you allow messages between different social networks, what you intended to be private can become public. For example, you might relate your Foursquare location to your public Twitter account and by doing this expose the message to the whole world [3].

Social media is used also by criminals for fraud, gathering business intelligence, stealing sensitive information etc. Social media security risks include [4]: insufficient authentication controls, cross site scripting, cross site requestforgery, information leakage, injection flaws, information integrity, and more. The main cyber-attack methods are: Spear Phishing, Social Engineering and Web Application Attacks. Spear Phishing is anattack which targets a specific user or group of users, and attempts to deceive the userinto performing an action, such as opening a document or clicking a link, that launchesan attack [5]. The use of abbreviated URLs on sites likeTwitter makes it easy for cybercriminals to mask and direct users to malicious web sites.Social Engineering, which relies on exploiting the human element of trust [6], obtains or compromises information about an organization or its computer systems [7].Social media sites such as Facebook provide the ability for a user to maintain his or herown web page and share content with their personal connections. By breaching the trusta user has with his or her online network, hackers are able to embed malware into friends’content and cause yet more people to fall victim to the malicious link [8]. Recent advances in Web Application technologies allow attackers to usenew techniques to target users [9]. For example, a user may grant a maliciousweb application access to his or her Facebook account, which may compromise theaccount or may download unauthorized software to the user’s computer.

As long as social media sites share information with other social media sites, location-sharing is allowed and people are becoming comfortable with disclosing such information, then anyone will readily be able to get sensitive information. Combine this with overly enthusiastic users, who intentionally or not, share too much personal information and developers who can access private information, then social media presents a very severe security risk [2].

There are several mitigation techniques to reduce social media security risks [4]. Many organizations have developed a formal policyto guide employees' use of social media. A formal policy usually containsguidelines that specify what is the acceptable use of social media and what is not acceptable,what information employees can share and cannot share, consequences of non-compliance,legal or regulatory requirements related to social media content, corporate supportbrowsers and configurations, privacy settings, password policy, etc. [10]. For example, the guideline may ask the employees to use acorporate supported browser and use strong passwords for socialmedia sites that are not thesame as any credentials used within the enterprise. But policies and guidelines are not enough. Even if the employees are aware of the policy, most chances that they won't know how to implement it in real cases. We need complementary layers: education, training and technology means.

When an organization is attacked because of a human error, it is customary to say that humansare the weak link in the chain. A report by IBM released on 2014 attributes some 95% of IT security breaches to human error [11]. Since the attacks have many layers, the human factor in social media should be handled in several layers as well. These layers can be gathered into two important aspects: education& training and technology. The following sections will elaborate on these aspects.

2. Education and training

If the humansare the weak link, we should strengthen it, and the first stepis education. The internet at its first stages was used by the academy and then worldwide as a large knowledge database. Business and applications for youth were soon to come. Today also young children are exposed to the internet for gaming, online learning etc. But the internet has risks even for this age, for example cyber-bullying, pedophilia, accessing adults' sites etc. So cyber education should start as early as the first grade, to protect the children at their first steps in the cyber world. Teaching the risks of the online media and the ways handling them should become part of the formal school lessons. In the high school the lessons should be expanded to include more aspects relevant to the youth. Starting to teach the childrenthe cyber risks and the precautions when they are young will also raise the chances that caution will become their nature when they grow up.

Proper training can raisesecurity awareness and personal responsibility in order to help prevent social mediasecurity incidents, such as malware and data breaches [10]. Organizations should provide effective security awareness training toemployees on a regular basis. Security awareness training should provide detailedexplanations of the organization’s social media acceptable use and security policy,examples of various social media attacks, and emphasize proper precautions tomitigate the security threats and risks, as well as the reporting of security incidents. The reported security incidents are good examples for the next training session, because they provide relevant cases studies to illustrate social media risks specific to the organization. To raise the chances that secure use of social media becomes a habit, updated trainings should be held in a periodical manner, including relevant case studies, which should be illustrated and implemented with hands-on sessions.

An unusual and interesting approach to cyber security training is using video games[12]. Although many of the concepts included in cyber security awareness training are universal,such training often must be tailored to address the policies and requirements of a particularorganization. In addition, many forms of training fail because they are routine and donot require users to think about and apply security concepts. A flexible and interactive video game can support organizationalsecurity training objectives while engaging typical users in a security adventure.

An important part of training is ongoing improvement, which can be achieved by evaluating the trainingsessions and measure their effectiveness. Training evaluation can be done by the classical ways of tests and evaluation forms. An effective evaluation method can be utilizing drills – simulating actual social engineering on the employees to see if they recognize the attempt, if they fall in the trap and if they report the incident. Such an unannounced drill was conducted in the US Military Academy [13], in which they evaluated users' propensity to respond to email phishing attacks. The results showed that the students continued to disclose information that should notbe disclosed to an unauthorized user and exposed themselvesto malicious code by opening attachments.

3. Technology

Education and training are only one aspect of defending against cyber-attacks. The second main aspect for overcoming human errors is technology: putting more effort on technologicalmeans of helping humansmake fewer errors and avoid falling into cyber traps. Since one of the first steps of a social engineering scam is collecting information on the target, and social media can be a fertile ground for such information, the first step of security in the social media is privacy settings to limit access to the user's information.

Organizations should ensure that up-to-date firewall, antivirus and antispywaresoftware are installed on employees’ computers and other devices they use [10].It is important for employees to understand the importance of performing regularscans not only of their computers/devices, but also of any file they download from aweb site, email, or flash drive.

Social media site monitoringtools such as Google Alerts and Social Mention can help organizations keep track ofmalicious activities and threats against the organizations that attackers sometimesdiscuss publicly [14]. These tools often provide email alerts and RSS feeds tokeep organizations updated if the organizations' names are mentioned on social media.

Another risk in social media is fake identities – younever know who stands behind a friendship proposal. One of the serious faults in social media is accepting friends without filtering. Technology can help here to check the reliability of the person suggesting friendship, by checking his personal details and cross-check it against open databases and other users' references.When having many friends in the social media, the risk continues by those friends trying to gain trust. Since people tend to accept content more easily from trusted friends, we should use technology to auto-check every link and every piece of content sent to us, to make sure they are not malicious. This can be achieved by checking of known malicious sites and running received content in a sandbox.

The other side of the coin is: can we use social networks to identify an organization's weak link – the insider threat? If someone in an organization is leaking business information deliberately, there are many ways to handle this threat: detecting the action, using technological means to prevent it etc. Another way of tackling such threats is using social networks to predict the intention of someone to harm his employer.

The information in the social media can reveal precursors, such as social and personal frustrations, anger or will to take revenge, reduced/dividedloyalty, narcissism, predisposition towards law enforcement etc. As described in the Security Project (2014) [15], there are different behavior prediction theories that may predict different precursors. It is shown that by analyzing 2 million comments on 200,000 videos in YouTube, predisposition towards law enforcement was predicted with 80% accuracy, and divided loyalty was predicted with 87% accuracy.

Palo Alto Research Center (PARC) researchers have set up on 2012 a number of experiments to observe potential insider threat behavior in closed online environments [16]. They looked at the massively multiplayer online game World of Warcraft. The game allows users to build characters, join large organizations called guilds, and go on missions and assignments. Players hunting dragons and orcs wind up collaborating with team mates, applying for positions and earning rewards in somewhat the same way that work teams go about tackling big projects. The game thus served as a suitable proxy for a real world work environment [17].The researchers found that they could predict who was going to quit in six months in advance with an accuracy rate of 89%. After expanding the research to the real world, they found some important clues that can predict potential insider threat behavior. The best attrition symptom was fewer emails, fewer messages after hours, fewer attachments, and fewer words all together. It seems that the potential malicious employee in the organization may be the guy going dark. According to the researchers, the model could scale up to apply to virtually any domain where online social interaction can be observed and measured.

4. Summary

The digital era changed the way we communicate. Social media became the place we share our experiences, opinions, statements etc. But the social media has inherent security risks. To strengthen the human factor, we should put effort in education, starting at school, through college, continuing with organization trainings, including relevant case studies, which can be best illustrated and implemented with hands-on sessions, until secure use of social media becomes habit. Unusual approaches to cyber security training should be considered, such as interactive video games. To ensure ongoing improvement, training should be evaluated to measure their effectiveness, for example by simulating actual social engineering on the employees, such as email phishing attacks, and to see if they recognize the attempt or if they fall in the trap.

But we should not rely only on education and training, but putting more effort on technological means of helping human make less errors and avoid falling into cyber traps. This can be initiated with enforcing privacy settings to limit access to the user's information. Social media site monitoring tools can help organizations keep track of malicious activities and threats against the organizations that attackers discuss publicly. Technology can also help checking the reliability of a person suggesting friendship in social media, to make sure he is a reliable person. Social networks can be used also to identify an organization's insider threat, by analyzing the social media content to predict the intention of someone to harm his employer.

Each of the mentioned aspects is important, but they complement each other. So combining education and training with best-of-breed technology may be the best way to mitigate social engineering risks and reduce potential damages.

References

[1] P.B. Brandtzaeg, J. Heim, Why People Use Social Media Sites, Lecture Notes in Computer Science Volume 5621, 2009, pp. 143-152
[2] C. Rose, The Security Implications Of Ubiquitous Social Media, International Journal of Management & Information Systems – First Quarter 2011, Volume 15, Number 1
[3] F. Groeneveld, B. Borsboom, B. van Amstel, Over-sharing and Location Awareness, Center for Democracy & Technology, 2010, February, www.cdt.org/blogs/cdt/over-sharing-and-location-awareness
[4] Wu He, A review of social media security risks and mitigation techniques, Journal of Systems and Information Technology, Vol. 14 No. 2, 2012, pp. 171-180
[5] M. Jakobsson and S. Myers, Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft, Wiley, Hoboken, NJ. 2006
[6] S. Granger, Social Engineering Fundamentals, Part II: Combat Strategies, 2002, www.securityfocus.com/infocus/1533
[7] S. Abraham and I. Chengalur-Smith, An overview of social engineering malware: trends, tactics, and implications, Technology in Society, Vol. 32 No. 3, pp. 183-96, 2010.
[8] M. Huber, S. Kowalskiy, M. Nohlbergz, and S. Tjoa, Towards automating social engineering using social networking sites, Proceedings of International Conference on Computational Science and Engineering, 2009
[9] CDC, Social Media Security Mitigations, 2009 www.cdc.gov/socialmedia/tools/guidelines/pdf/securitymitigations.pdf
[10] M. Chi, Security policy and social media use, 2011, www.sans.org/reading_room/whitepapers/policyissues/reducing-risks-social-media-organization_33749
[11] F.J. Ohlhorst, www.techrepublic.com/article/ibm-says-most-security-breaches-are-eue-to-human-error, October 2014
[12] B.D. Cone, C.E. Irvine, M.F. Thompson, T.D. Nguyen, A Video Game for Cyber Security Training and Awareness, Computers & Security 26 (2007), pp. 63-72, Elsevier
[13] R.C. Dodge Jr., C. Carver, A.J. Ferguson, Phishing for user security awareness, Computers & Security 26 (2007), pp. 73–80, Elsevier
[14] L. Zeltser, Monitoring social media for security references to your organization, 2011, isc.sans.edu/diary.html?storyid=10921
[15] D. Gritzalis, Holistic Information Security: Human Factor and Behavior Prediction using Social Media, www.infosec.aueb.gr/Publications/Security Project 2014.pdf, January 2014
[16] O. Brdiczka, J. Liu, B. Price, J. Shen, A. Patil, R. Chow, E. Bart, N. Ducheneaut, Proactive Insider Threat Detection through Graph Learning and Psychological Context, Palo Alto Research Center, 2012, www.parc.com/content/attachments/proactive-insider-threat-detection.pdf
[17] P. Tucker, How Big Data Could Help the U.S. Predict the Next Snowden, February 2014, www.defenseone.com/technology/2014/02/how-big-data-could-help-us-predict-next-snowden/78671/