THE DARK SIDE OF SOCIAL NETWORKING SITES: UNDERSTANDING PHISHING RISKS

Pre-print

To cite:
Mario Silic, Andrea Back, The dark side of social networking sites:Understanding phishing risks, Computers in Human Behavior, Volume 60, July 2016, Pages 35-43, ISSN 0747-5632, http://dx.doi.org/10.1016/j.chb.2016.02.050.

Mario Silic, Andrea Back
mario.silic@unisg.ch

Institute of Information Management, University of St.Gallen, 9000 St.Gallen, Switzerland

Abstract:

LinkedIn, with over 1.5 million Groups, has become a popular place for business employees to create private groups to exchange information and communicate. Recent research on social networking sites (SNSs) has widely explored the phenomenon and its positive effects on firms. However, social networking's negative effects on information security were not adequately addressed. Supported by the credibility, persuasion and motivation theories, we conducted 1) a field experiment, demonstrating how sensitive organizational data can be exploited, followed by 2) a qualitative study of employees engaged in SNSs activities; and 3) interviews with Chief Information Security Officers (CISOs). Our research has resulted in four main findings: 1) employees are easily deceived and susceptible to victimization on SNSs where contextual elements provide psychological triggers to attackers; 2) organizations lack mechanisms to control SNS online security threats, 3) companies need to strengthen their information security policies related to SNSs, where stronger employee identification and authentication is needed, and 4) SNSs have become important security holes where, with the use of social engineering techniques, malicious attacks are easily facilitated.

Keywords: social networking sites; field experiment; deception; employee psychology

I. INTRODUCTION

From the late 1990s, when the first website enabling user profiles to be linked appeared, to today, the number of social networking sites has increased significantly (Boyd & Ellison, 2007). The addition of new features, enhancements and innovations leveraged further social networking site (SNS) usage and its appeal for firms. From an individual and organizational perspective, SNSs became very popular as the preferred place to communicate and collaborate (Kuikka & Äkkinen, 2011; Szwedo, Mikami, & Allen, 2011). One such successful example is LinkedIn, a popular professional SNS, which in 2013 had more than 1.5 million Groups, of which 900,000 required membership access. On the one side, SNSs provided employees with the tools and technology to connect and interact with each other and, on the other side, they enabled positive contributions to firms in terms of facilitating and leveraging a collaborative corporate culture. However, SNSs are growing more rapidly than organizations' ability to monitor and manage these new communication channels. A recent survey from Proofpoint found that an average Fortune 100 company has 320 authorized social media accounts, but 40% of the Facebook accounts claiming to represent a Fortune 100 brand are unauthorized (Proofpoint research, 2014). In the SNS context, where the employee is the key component, research shows that the main weakness in properly securing organizational information systems is the employee (Posey, Bennett, & Roberts, 2011; Stanton, Stam, Mastrangelo, & Jolton, 2005; Warkentin & Willison, 2009). Moreover, nearly half of the intrusions and security breaches are caused by organizational insiders (Baker et al., 2011; Richardson, 2008). It is clear that employees represent an important aspect in the organizational information security intrusion/detection systems. The impact on firms can be very high, in terms of financial loss but more importantly, risk related to reputation (Blakley, McDermott, & Geer, 2001). Furthermore, online large-scale networks (e.g. LinkedIn, Facebook, Twitter) have raised a number of important privacy issues, as employees can use these SNSs to store some sensitive and confidential data. According to (Malik & Malik, 2011), disclosing and sharing private information is a necessity in order to be visible on SNSs, but at the same time, malicious attacks can be largely facilitated thanks to the data disclosures. It seems that the awareness of these threats is very low among users and, generally, users do not really care about the possible implications and risks associated with data sharing (Donath, 2007; Jagatic, Johnson, Jakobsson, & Menczer, 2007; Light, McGrath, & Griffiths, 2008). With the expansion of SNSs, combined with the lack of efficient and established controls (Proofpoint research, 2014; SANS, 2012) we are witnessing an increased number of security incidents related to the exploitation of the human factor on SNSs (PwC, 2014a, 2014b). The technique most widely used by attackers that focuses on the human element is commonly called social engineering. It is defined as the art of deceiving or tricking people to help attackers reach their goals, to gain information from them, or to persuade them to perform an action that will benefit the attacker in some way (Mitnick & Simon, 2001). Phishing is another form of social engineering in which the attacker attempts to fraudulently retrieve legitimate users' confidential or sensitive information by mimicking electronic communication from a trustworthy source (Jakobsson & Myers, 2006). A survey from Kaspersky's lab found that the proportion of spam in email has decreased by 2.5% from 2012, yet still represented 69% of the 507 billion emails sent per day in 2013. The survey also revealed that phishing attacks are shifting from bank accounts to social networking and email (Kaspersky, 2013). Despite the fact that phishing is a relatively familiar nuisance, phishers often successfully steal sensitive information (Ryan T. Wright & Marett, 2010). One recent example is the phishing attack against Target, which led to the exposure of 110 million consumers' credit cards and personal information (Harris, Perlroth, Popper, & Stout, 2014). The risks posed by phishing attacks for firms range from financial losses (Cohen, 2013; Hong, 2012), corporate and industrial espionage (Grow, Epstein, & Tschang, 2008), and stealing classified and private information (Hesseldahl, 2011) to revealing organizational secrets (Healey, 2013) or putting companies' reputation at risk (Blakley et al., 2001). Despite the fact that firms have implemented numerous technical solutions to mitigate the risks behind phishing, such as the detection of fake websites (Abbasi, Zhang, Zimbra, Chen, & Nunamaker, 2010) or the use of warnings (Egelman, Cranor, & Hong, 2008; Silic, 2016; Silic, Barlow, & Ormond, 2015), it was found that phishing attacks remain rather successful because they are generally performed in legitimate communication channels, which makes them difficult to distinguish from genuine messages (Dhamija, Tygar, & Hearst, 2006) .

Although many researchers have investigated the risks associated with phishing in SNSs (Algarni, Xu, Chan, & Tian, 2014; Chitrey, Singh, & Singh, 2012; Hogben, 2007; Jagatic et al., 2007; Nagy & Pecho, 2009), and have highlighted the fact that SNSs represent the most common source of phishing attacks, fewer have examined how employees respond to phishing attacks and how organizations are dealing with the associated threats. Indeed, most of the past studies used non-business user populations to investigate the phishing phenomenon. For example, Jagatic et al. (2007) launched a phishing attack via email that targeted university students in order to better understand how they react when phishing emails are sent by friends rather than an unknown person. Interestingly, Facebook was used in several studies to understand how deception affects users. One study used Facebook users to investigate how they distinguish between attackers and legitimate users based on their characteristics (Algarni et al., 2014). Vishwanath (2014) studied farcing attacks on Facebook (the phisher uses victim's social media page to conduct the attack) and found that social contagion effects are largely facilitating the diffusion of deception in the social media context. More recently, Facebook habits and its determinants were studied to understand how they influence individual susceptibility to social media phishing attacks (Vishwanath, 2015). Clearly, people who habitually use Facebook are significantly more likely to fall victim to the SNS phishing attack (Vishwanath, 2014). Studies on deception in SNSs have contributed to a better understanding of the user's identity by investigating their profiles (Al Zamal, Liu, & Ruths, 2012; Alowibdi, Buy, Yu, & Stenneth, 2014; Liu & Ruths, 2013) in order to classify users' based on their characteristics such as gender. Several studies focused on how to detect spam in SNSs (Castillo, Mendoza, & Poblete, 2011; Chu, Gianvecchio, Wang, & Jajodia, 2012) by investigating user's profiles to discover if it was human created or not. However, as social engineers are usually humans, these previous findings are rather limited when applied to social engineering attacks (Algarni, Xu, & Chan, 2015).

Overall, past studies mostly used email as the phishing method, focusing either on students (Steyn, Kruger, & Drevin, 2007) or military cadets (Ferguson, 2005), to understand the effectiveness of phishing attacks, which could be a limiting factor, as business users are working in a different context, where various procedure or policies are usually already in place that may influence employees' online behaviors.

Furthermore, to defend and protect against phishing attacks, research suggests that education and training on security awareness could be quite effective (Luo et al., 2012). Also, clear and concise security protocols that would be enforced throughout the entire organization, where information sensitivity is clearly explained, is another countermeasure commonly implemented in firms (Gragg, 2003; Kvedar, Nettis, & Fulton, 2010). However, when it comes to the implementation of the countermeasures, empirical evidence is largely missing in terms of whether firms are really following what the research suggests and to what extent. Are employees really aware of the existence of education or training programs, and if so, are they following them? Another challenge is the difficulty to make accurate judgments regarding deception in the virtual environment of SNSs (Algarni et al., 2015) where user needs to decide about the credibility of attackers and consequently, to take a decision to accept or reject social engineering attacks (Algarni et al., 2014). Reason why people tend to be weak and perform poorly in detecting deception can be found in the "lie detector bias", which assumes that most people are telling the truth (Marett, Biros, & Knode, 2004). However, in the organizational context, employees are usually well trained and should be less susceptible to that bias. But, it seems that in reality employees are mixing the professional and private personas. Skeels and Grudin (2009) when studying the workplace use of Facebook and LinkedIn, found that private and professional roles are often mixed which can bring some information security challenges as employees have difficulties in adapting the content they place on SNS when switching from one to another role.

Thus, the challenge related to the past studies is that they were not studying business users, but were instead focused mostly on students or general Internet users (e.g. Facebook users). This can be explained by the fact that access to data can be very difficult, as firms may not be open to collaboration that would provide access to study the phishing phenomenon for security and privacy reasons. We believe that the business context is an important aspect to investigate as it may provide new insights about the complex relationship between the human factor (i.e. employees) and the phishing attacks, which may lead to a better mitigation of the underlying risks for organizations in SNSs. Indeed these risks can be two-fold: 1) personal and 2) organizational risks. On the personal level, attacks usually result in identity theft which enables attacker to proceed to the next steps in the attack process (e.g. use victim's

identity to penetrate into organizational systems). Organizational risks range from reputational risks, loss of high-value organizational data to financial losses. Our manuscript contributes to the understanding of these risks and the effects of phishing by suggesting that existing organizational SNS policies and procedures are not adequate and should be adapted to SNS realities. More precisely, stronger employee identification and authentication is needed in combination with updated, clearer and more robust information security policies related to SNSs. Also, we suggest that the security awareness, educational and training approaches should be revised by incorporating SNS specifics such as risks of 'liking' individuals where checking the legitimacy of the friend's request should be mandatory.

Overall, while SNSs are presently used by employees to conduct positive activities online (e.g. collaboration), there is also a negative side: they can be a perfect target for attackers to exploit online collaboration and gain valuable information that can be used for malicious activities. We argue that there is a gap in the current understanding of this negative side. Despite several studies that dealt with SNS and phishing attack risks, we believe that the business context has not been adequately studied thus far. We aim to close the existing research gap by exploring the following research questions:

How do employees respond to phishing attacks on SNSs?

How are firms coping with threats related to phishing attacks?

Supported by the credibility, persuasion and motivation theories, to answer these questions, we conducted an online field experiment followed by interviews to better understand the underlying relationships between SNSs dynamics and phishing attacks.

The paper is organized in the following way. Firstly, we establish the theoretical background, followed by the presentation of the research methodology, outlining data collection and analysis. Then, we discuss the findings of the study. Finally, we conclude by providing suggestions for future research and implications for practitioners, as well as highlighting the limitations of this study.

II. THEORETICAL BACKGROUND

Attackers will often use a contrived situation or personal persuasion to increase the chances of their request being successful (Parsons, McCormac, Butavicius, & Ferguson, 2010). They rely on the credibility phenomenon, which is a communication process happening between two parties (Eisend, 2006). Credibility originates from persuasion, which is built upon three elements: the source, the message and the recipient(O'Keefe, 2002). In the SNS context, the source is the attacker, the message is the technique used by the attacker (e.g. phishing) and the recipient is the victim (e.g. employee). Interestingly, users claim to be concerned about privacy risks when using SNS, but, at the same time, do little to safeguard their information (Dwyer, Hiltz, & Passerini, 2007). This behavior is partly explained by the desire for social interaction which outweighs their concerns about privacy and disclosure of personal data (Debatin, Lovejoy, Horn, & Hughes, 2009). For Rosenblum (2007, p. 47) SNS users "don't exercise the same common sense because they conceive of themselves as interacting in a protected environment". To make the phishing attacks realistic, attackers mimic the content of legitimate messages (Ryan T. Wright & Marett, 2010) and try to build content that would look genuine and authentic. In order to increase believability, attackers customize the content of their message (e.g. personalizing email messages or reproducing websites that look identical to the target site) to increase chances of being trusted by the recipient. Also, the credibility can be heavily influenced by the use of additional cues (e.g. logo, graphics, etc.), encouraging the victim to perceive the other party as more credible, thus beginning the communication process (Dhamija et al., 2006). However, believability is generally not enough to trigger an interaction between the two parties. Attackers will have to use various influence techniques to build a trusting relationship. One such influence technique is the use of connections or friends, where attackers pretend to be part of the victim's network (Jagatic et al., 2007). Particularly in the SNS context, this may be very relevant, as SNSs are built on the 'networking' concept and 'being a friend of a friend' may result in a higher likelihood of being accepted. For example, when a new company employee joins LinkedIn and sends a request to join his or her company's private group, the employee may be given group moderator

approval much faster than someone whose LinkedIn profile does not show his or her company's affiliation. Additionally, it was found that users may make different decisions when it comes to different situations. If they are asked to wire an amount of money or engage in financial transactions, users usually become more suspicious and question the validity of such requests (Jakobsson, 2007). However, if an attacker is recommending that users visit a fabricated website and perform certain actions, this usually results in the loss of private information (Conti & Sobiesk, 2010). Some influence techniques were found to be more effective than others. Specifically, phishing influence techniques that relied on fictitious prior shared experience were found to be less effective than techniques offering a high level of self-determination (Ryan T Wright, Jensen, Thatcher, Dinger, & Marett, 2014). Overall, influence techniques, supported by persuasion and motivation theories, can be split into six different categories: liking, reciprocity, social proof, consistency, authority, and scarcity (Cialdini & James, 2009). Liking is particularly interesting in the SNS context, as the employees tend to say yes to people they "know and like" (Cialdini & James, 2009, p. 142). However, research did not come to any strong conclusions about which techniques are the most effective (Sundie, Cialdini, Griskevicius, & Kenrick, 2012). In that context, it seems that each technique's effectiveness is result of the context and the way in which it is employed (Ryan T Wright et al., 2014). Consequently, we have little insight into which technique will be the most effective in a phishing context where we have no clarity on the message source (Ryan T Wright et al., 2014).

This is particularly true in the SNSs context, where employees generally think that they can easily identify and avoid phishing attacks. However, research showed that people have difficulty identifying lies and persuasion techniques (Grazioli, 2004; Marett et al., 2004). Moreover, if the victim believes that his action or inaction will have important consequences, attackers are more likely to succeed (Gragg, 2003). Workman (2008) defines this situation as affective commitment, where users that feel an attachment or emotional bond to the phisher will more easily divulge sensitive information. This is also supported by Cialdini and James (2009) who argue that once users have made a decision, they can feel pressure to be consistent with their choice and not change it. This leads to a situation where people act in ways that are contradictory to their interests. This situation is referred to by Workman (2008) as normative commitment, which is an extension of the idea of reciprocation. This technique, called reverse social engineering, is used by attackers to create a problem and then offer to assist victims.

Interestingly, only a small number of studies have attempted to provide empirical evidence of how people respond to social engineering attacks (Parsons et al., 2010). The majority of these studies used student populations to understand the effectiveness of such attacks. Also, Algarni et al. (2014) argues that "there is a severe lack of research dedicated to the susceptibility of social engineering victimization in SNSs". While the susceptibility to security victimization related to the employees' compliance with organizations' security policies was widely studied through different theoretical lenses using protection motivation theory (Johnston, Warkentin, & Siponen, 2015), technology threat avoidance theory (Herath et al., 2014) or routine activity theory (Wang, Gupta, & Rao, 2015), studies that dealt with susceptibility to specific types of SNS phishing attacks are still relatively scarce. This is partly explained by the complexity related to the data collection process where employees and organizations are usually reluctant to participate in such studies. Overall, current knowledge on how employees respond to phishing attacks in the SNS context needs to be further investigated. Establishing a better understanding of this relationship would not only broaden knowledge, but also provide guidance for firms in terms of helping their employees better recognize and avoid the threats behind SNSs use. Indeed, the deception theory (Carlson & George, 2004) suggests that pre-interaction factors (e.g. individual characteristics or context) are highly important in explaining behavior during the deceptive interactions. Hence, employees context can produce quite different results when compared to, for example, Facebook users. Similarly, email communication context is likely to impact user's behaviors in a different way than SNS context. This clearly raises brings some challenges to studies dealing with social engineering as pre-interaction factors seem to play an important role in the deceptive interactions. For example, e-mail based phishing attacks usually require several communication exchanges, while in the SNS context, using, for example, the 'liking' approach, the communication process is usually limited to one way communication where attacker will become 'friend' in a much fast way. This adds another challenge for SNS phishing risks as detection of deceptive intent of the 'friend request' becomes much hard and more complex.

Previous studies on how to minimize social engineering risks to information security showed that there are four main reasons why countermeasures through automated security tasks cannot solve the problem (Ong, Tan, Tan, & Ting, 1999; Ruighaver, Maynard, & Chang, 2007). These reasons were categorized by Workman (2008) into four categories: 1) financial, 2) situational, 3) cultural, and 4) technological. Instead, organizations mostly rely on security awareness and training, which are considered to be the most effective countermeasures against human factor threats to information security (Parsons et al., 2010). Another method suggested by Mitnick and Simon (2001) is "auditing and testing", which consists of testing employees' susceptibility to social engineering-based attacks. However, we are missing some insights about the effectiveness of these methods in the business context. Namely, are employees aware of the existence of any training materials, and if so, are they providing the necessary guidelines for how to behave in the SNS context?

III. METHODOLOGY

Our study used a mixed approach. Firstly, we conducted a field experiment in a Fortune 500 company (Financial services) with the aim of understanding how social engineering techniques can be used by an attacker to become a SNS private group member and, subsequently, obtain data from company employees. For this experiment, we created a fake website, inviting employees to visit it (see below for details). Secondly, a qualitative study of employees (who were in the scope of the field experiment), was conducted using interviews. Finally, we interviewed the Chief Information Security Officers (CISOs) from 11 different organizations in order to obtain answers to our research questions.

Field experiment

We performed an initial study that was conducted and designed as a field experiment, as we wanted to have stronger study validity and because our aim was to generalize our findings for further use by practitioners. For the purpose of our study, we focused on a company that granted us permission to conduct a simulated attack. This organization is a Fortune 500 company with offices all around the world. Also, the number of company users participating in online social interaction exceeded 8,000. We launched a harmless attack with the objective of getting some general data, without trying to obtain any sensitive data. We wanted to stay generic, as getting sensitive data would have raised ethical issues that we wanted to avoid. All ethical concerns and challenges were previously discussed and agreed to by the company's ethical department and our institution. We also received written authorization to proceed with our study. We began by creating a fake online profile on the SNS that we identified as the Target. The profile included fake information identifying the attacker as an employee of the company. Furthermore, the attacker sent 100 invitations to 'network friends' and waited until at least one of the contacted employees accepted. Thirty-five requests were accepted. Next, access to a private discussion forum with 1,200 members (hosted on the Target SNS, with only company employees having access to it) was requested. The private group moderator accepted the request without any formal verification. From that moment, the attacker was a member of the private discussion forum and could engage in discussions with actual employees. Targets were selected based on different criteria, such as the quantity of publicly available information and their professional experience and background. They were further divided into different categories representing typical social engineering victims.

The process for the control group was the following: 1) we created a fake online profile on the SNS with the profile identifying the attacker as a student; 2) we sent 40 invitations to company employees. We received two acceptances. Finally, we requested access to the private group, but were rejected. A follow-up email was sent to the group moderator to inquire about the refusal. Only after explaining that we were doing an internship for the company were we granted access.

It is important to note that the entire field experiment was carefully coordinated and managed with company's IT security department to ensure that 1) all ethical procedures were strictly respected and that 2) the experiment would be successful. Moreover, one of the researchers who conducted the entire attack had solid knowledge of social engineering techniques and paid particular attention to the entire study protocol to make sure that the entire approach avoided any ethical dilemmas.

The design of the experiment was based on collecting non-sensitive information from company employees. The information was more technical in nature, but still generic enough not to reveal any potentially sensitive data.

To launch the attack, the researcher posted a link to the group wall, inviting employees to participate in a new beta test project in which several pieces of information were asked for from the employees, such as their email address, office location, age, name, and function. The link then led employees to an external web page (specially created for the research). A similar approach was used for the control group, but instead of posting a link to the group wall, we directly contacted 35 employees through the messaging feature within LinkedIn. This is because we did not want to be identified as a company employee, but rather as a student, since we did not want to influence employees' decisions. The results from this initial study are presented in the findings section.

Interviews

We conducted 21 semi-structured interviews between February and April of 2014. All interviewees were employed by the company. We had two different groups of informants. On one hand, ten employees (users of SNSs and not involved in the field experiment) were interviewed, as we wanted to understand their views on the threats and challenges posed by SNS use, what kind of mechanisms and procedures they were aware of, and what, in their view, was effective and what was not. Moreover, employees could provide valuable information on the internal procedures and processes in order to understand how SNSs are perceived from a security standpoint. We also interviewed 11 informants who were all Chief Information Security Officers (CISOs) from 11 different organizations. All of the interviews lasted between 37 and 45 minutes (on average 41 minutes), resulting in a total of 77 pages of transcribed text. Most of the employees' interviews were much shorter in duration as compared to the CISOs, as the employees generally had much less knowledge regarding security challenges.

The qualitative interview followed an interview guideline, which was developed with the help of an external security expert who had relevant security experience regarding SNSs. Given that we had two different groups, we also had two versions of the guideline. The guideline was designed using open-ended questions. For employees, it related to the following areas: employee perception of SNSs, knowledge of the security policy/training, awareness of threats, effectiveness of previous training, and the online security policy. For CISOs, slightly different aspects were discussed: online threats, existence of internal mechanisms to control employees, external vs. internal online threats, existence of countermeasures, and security procedures. As several informants did not want to be identified, we kept both employee and CISO replies anonymous. The employees' interview were coded E1 to E10 and CISOs as C1 to C11.

To better preape all interviews, we explained in detail to all participants the results of the initial online field experiment study (see findings section for more details). This approach had been previously used by Jagatic et al. (2007).
Table 1 summarizes our sample characteristics.

Characteristics	Age	(%)	*Gender*	Number (N=21)	(%)
< 20	1	4.7%	Male	12	57.2%
20-30	6	28.5%	Female	9	42.8%
31-40	6	28.5%			
> 40	8	38.3%			

To gain more insights on social network websites and their challenges to organizations, we used interviews as the research method. People from 11 organizations and six different countries were

interviewed. We picked both private and public organizations, with different sizes and numbers of users served by their IT departments. We believe this gave us a solid diversity of organizations in our sample.

The characteristics of the interviews are presented in Table 2.

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
Type	Private	Private	Public	Private	Public	Private	Public	Private	Private	Public	Public
Industry	Financial	Financial	Gov.	IT	Insurance	Consulting	Bank	Financial	IT	Gov.	Gov.
IT dep.	Central	Central	Decen.	Central	Central	Decen.	Central	Central	Central	Central	Decen.
Size	250	80	1200	115	20	550	25	105	75	110	38
Nb.Users	1100	950	30000	1050	430	16900	750	680	2250	4790	1140

To analyze the interviews, we used the NVivo software program (version 10). Our study utilized exploratory analysis, as suggested by Creswell (2002), and we analyzed the data by reading through all of the transcripts, quickly identifying and highlighting the ideas in order to get the big picture. The NVivo program further enabled us to visually code different patterns, data, phrases and words so that we could group them into defined categories and themes. In this preliminary analysis, several themes emerged that were further analyzed and which are discussed in following sections. Finally, common themes were interconnected, and we extracted different levels of abstraction as per Creswell's suggestion (Creswell, 2002).

IV. FINDINGS

Firstly, we conducted a field experiment, as we wanted to understand how employees respond to phishing attacks on SNSs and more precisely, if contextual elements play a significant role in deceiving employees.

Overall, our research reveals that 1) employees are easily deceived and susceptible to victimization in SNSs where contextual elements provide psychological triggers to attackers, 2) organizations lack the mechanisms to control SNS online security threats, 3) companies need to strengthen their information security policies related to SNSs, namely in the form of stronger employee identification and authentication, and 4) SNSs have become important security holes where, with the use of social engineering techniques, malicious attacks can be easily facilitated. Moreover, our field experiment confirms that employees completely lack security training related to awareness, risks, and threats of SNSs.

Field experiment findings

We received 180 visits on the webpage created for this study. Of these visits, 122 employees (68%) filled in the fake webpage information, while 15 others started, but did not finish.

Characteristics	Age	(%)	*Gender*	Number (N=122)	(%)
< 20	10	8.1%	Male	55	45.1%
20-30	55	45.1%	Female	67	54.9%
31-40	28	22.9%			
> 40	29	23.9%			

From Table 3, we can see that females were more likely to become victims (54.9%) and overall, the younger population (aged 20-30) represents the most vulnerable category. We also contacted 15 employees by email to learn why they did not complete the web page form; all of them stated that 'something was wrong with the web page – it did not look genuine', so they gave up. Examining the website logs to better understand the temporal dynamics, we found that employees visited the fake webpage in the first hour after the link was posted on the discussion forum.

From the information provided by the 122 employees, we can see the following function distribution: call center (41.8%), marketing (8.1%), finance (9.0%), IT (4.1%), management (18.0%), HR/Legal (9.8%), and Sales (9.2%). It appears that those who work in call centers are the most vulnerable to social engineering attacks, followed by management.

The online experiment was stopped after five days, after which we contacted all 122 employees by email, informing them about the study and providing them with another link to anonymously provide their feedback.

Regarding the control group, out of 35 contacted employees asked to click on the link, we had only 3 successful attempts (9%) where employees clicked on the link and identified themselves.

Results of the experiment (SNS and control group) can be found in Table 4.

	Targeted	Successful	Percentage
SNS	180	122	68%
Control	35	3	9%

Furthermore, ten employees accepted our invitation to be a part of follow-up interviews. The next section deals with the interviews and case study findings.

Interviews and case study findings

Our interviews with the ten employees (not part of the field experiment) from the attacked organization and CISOs from 11 organizations revealed that: 1) organizations lack mechanisms to control SNS online security threats, 2) organizations need to strengthen their information security policies related to SNSs, namely stronger employee identification policies, and 3) SNSs have become an important security hole where, with the use of social engineering techniques, malicious attacks can be easily facilitated. Moreover, our field experiment confirmed that employees completely lack security training related to awareness, risks, and threats of SNSs.

Interview findings

Employee interviews revealed that: 1) employees have little knowledge of their company's existing policies regarding SNS use; 2) employees trust SNSs and are generally not aware of the potential security risks, and 3) security training regarding SNSs is not effective. Eight employees confirmed that, to the best of their knowledge, there is no security policy in place for SNSs. For E1, security training did not have any effect: *"…we have a number of different trainings on compliance, fraud, security…but they are quite generic...and honestly, I can't remember anything very practical…*" All employees clearly confirmed that they were aware of the security policy, as it is something that is regularly communicated to them. However, they confirmed that the existing security policy does not contain any SNS content: "*…I saw the policy and it was communicated several times by email…but how to use social media websites is not mentioned there…*" (E6). We explained to all the employees how we conducted our online laboratory experiment, and as all of them were 'victims', we received confirmation from all of them, except E3 and E5, that they were not aware of the 'social engineering' risks and its implications. Two informants (E3 and E5) said that they do have some knowledge of the security risks, but for them, the issue is that when you are using SNSs, you tend to accept people's invitations in a 'blind way' without any verification.

CISO interview findings

In the following sections, we will detail the findings from the CISO interviews.

Lack of mechanisms to control external online security threats

Most of the CISOs recognized that their organizations do not seem to have any mechanisms in place to control online security threats: *"…no, we do not closely monitor online employee's activities. We do not have any tool, software or physical way to watch for the online threats…*" (C3). Usually, organizations do rather well when it comes to controlling internal information, but as soon as the border is crossed, it becomes very difficult to understand what is behind the organizations' security borders (C8, C10). The mechanisms are rather sporadic and there is no robust, well-defined and holistic approach for control or monitoring. Some organizations do have certain control mechanisms - *"…in some cases, yes. Agents running on the end-points.... some local logging.*" (C2) - and when employees are connected to their organization's network: "*Yes if they are over VPN connection, otherwise no, we do not monitor."* (C7). Two CISOs said that they could not discuss this, as it is quite a sensitive topic.

Inadequate Information Security policy

Seven of the 11 CISOs said that one of the biggest challenges is related to roles and responsibilities when it comes to maintaining the security policy related to SNSs: "*…there is lack of clarity when it comes to process owner…who should maintain the corresponding online security policy*" (C5). For CISOs, compliance and data privacy were found to be the top concerns that are inadequately treated through procedures and processes. "*…compliance is an important issue and if you want employees to be compliant they need to be aware and well educated."* (C4). Inadequate information security policies need to be brought up to date to deal with recent social media evolutions and adapted to our current social media reality. Five CISOs spoke about SNS evolution: "*…technology is evolving too fast…today you have one trend and in few months employees seem to switch to another one…"* (C11).

SNSs as a security hole

All 11 CISOs agreed that SNSs represent an important security hole – a bigger one than many might think. C6 pointed out: "*Social networks are more social than you think. In recent memory, between Facebook, LinkedIn, Twitter and Google+, more than five million account credentials (usernames & passwords) have been exposed/compromised. Given the rampant reuse of credentials across multiple applications and the ability to log into some other sites using your Facebook, Yahoo, etc. credentials, the resulting security risk is significantly great.*" In other words, the latest SNSs are proposing a password integration platform where the user can sign in with their Facebook password (Facebook Connect technology) to dozens of other applications. For C1, organization assets are easily compromised when using SNSs: "*inadvertent disclosure of company work, product, and secrets through posting of information*", while for C8, it represents an important security hole, as it is *"…a source of information for*

attackers to create convincing spear-phishing attacks." One interesting finding is that four organizations have already experienced attacks similar to the one we demonstrated in our online experiment. C4 explained *"…we had a bad experience…it was used to create fake identities as part of social engineering attacks…*" Information leakage, potential negative brand impact due to inadvertent posts, a source of information for attackers to create convincing spear-phishing attacks, and the inadvertent disclosure of company work, products, and secrets through the posting of information were found to be the most dangerous security holes for companies.

Security trainings

Effective training and education of employees received the highest attention from all informants. They all stated that educational awareness and training are the best strategies, and essential to leveraging information security. C1 said that it is not enough to have training and education; it needs to be more practical and more detailed: "*…Anti-Phishing awareness and sample exercises would be the best match as usually if it stays too generic people do not really care and do not pay attention…"* C4 did not agree with the importance of education and training, arguing that "*…people generally do not care…*", and saying "*the most effective way is to control it through software or hardware restrictions…essentially, not to leave it on the employee's shoulders.*".

II. DISCUSSION

Our research found that 1) employees are easily deceived and susceptible to victimization in SNSs where contextual elements provide psychological triggers to attackers; 2) organizations lack the mechanisms to control online SNS security threats, 3) companies need to strengthen their information security policies related to SNSs, namely in the form of stronger employee identification and authentication, and 4) SNSs have become important security holes where, with the use of social engineering techniques, malicious attacks can be easily facilitated. In the next section, we will discuss these four findings.

Firstly, our research extends current IT security research via an empirical examination of phishing attacks in the business context. To the best of our knowledge, this is the first empirical examination of phishing attacks in the business environment and the first analysis of how firms are coping with that phenomenon. Indeed, a recent study by Ryan T Wright et al. (2014) confirmed that the student populations used in most of the past studies is a limitation due to the participants' homogeneity. Given that our study focus was on employees who use LinkedIn for their professional social activities, we believe that it offers new insights on how employees react in such environments, as past research found that external SNS attacks do not seem to be a bigger threat to information security than other types of media (Hekkala, Väyrynen, & Wiander, 2012). Our findings are quite the opposite. When comparing the control group (employees that did not receive the treatment) to the SNS group, it is clear that the SNS group is much more susceptible to victimization of phishing attacks. We found that external attacks on the SNSs represent an important threat to information security for several reasons. The most important was the fact that today's SNSs enable users to use 'login platforms' (i.e. Facebook Connect), where users can log in to several other websites/applications using SNS login platform credentials. In that context, if the user's identity is compromised, not only is the corresponding SNS login compromised, but so are all the other websites/applications using the SNS's log-in technology. In its 2012 financial report,[1] Facebook reported that 600,000 accounts are compromised per day, and knowing that over 2.5 million websites use Facebook technology[2] to authenticate more than 250 million users[3] on their website in 2010, it could be argued that the information security threat coming from the SNSs is greatly facilitated and multiplied as compared to other types of media used for malicious purposes. Hence, this 'multiplication' effect can be seen as potentially very dangerous. Furthermore, contrary to past studies suggesting that attackers often use non-self-determined influence techniques (Lindsey, Dunbar, & Russell, 2011), we showed that the influence technique of 'liking' is particularly suitable to the SNS context and can be an important first step in the deception of employees. This is highlighted in the deception theory, which suggests that the pre-

[1] http://investor.fb.com/
[2] http://www.statisticbrain.com/social-networking-statistics/
[3] http://techcrunch.com/2010/12/08/250-million-people-now-connecting-via-facebook-connect/

interaction factors, such as context or individual characteristics, can facilitate and explain the deceptive interaction (Carlson & George, 2004). One interesting insight our study revealed is that little or no interaction is needed between the attacker and the victim, as the communication is facilitated by the SNS context. Prior studies argued that deception is based on the interactions between the attacker and the victim and is supported by repeated message exchanges (Carlson & George, 2004) where attackers adapt the message content to increase the likelihood of successful deception (Buller & Burgoon, 1996). However, in the SNS context, this message exchange or tuning is reduced to a minimum and often, is not needed at all, as then influence technique of 'liking' is used. Evidently, this increases the likelihood of being deceived, as attackers will have to spend less time in persuading the recipient. This also explains why we are seeing a recent trend of increased spam related to phishing attacks on SNSs (Kaspersky, 2013).

Secondly, we found that organizations do not have any efficient way of controlling and monitoring online security behavior resulting from their employees' online activities during working hours. Past research revealed that people often mix professional and private personas (Kuikka & Äkkinen, 2011; Skeels & Grudin, 2009), which seems to be an acceptable behavior, but also represents a major challenge for information security, as it appears that organizations ensure better information security when they can actively control the information flow (Hekkala et al., 2012). According to Li (2010), the way that social media services are monitored is very important, but the methods of how information and responsibilities should flow is also critical. Clearly, education and training represent an important method that organizations can use to train employees on how to resist phishing attacks (Luo et al., 2012). Moreover, developing clear security protocols with simple rules highlighting information sensitivity is another measure that should decrease the likelihood of being deceived (Gragg, 2003; Kvedar et al., 2010). Our research extends the previous findings, as we sought to understand if these suggestions are really in place within organizations. We found that there is a mismatch between what the reality is and how it should be designed. Organizations seem to lack the necessary mechanisms to control the external online SNS activities of their employees during working hours. We suggest that organizations maintain an appropriate level of information security to leverage the current responsibilities of the IT, legal or HR department, which would control all external SNS employee activities, or organizations should use 'intelligent software' to control social media activities.

Our research also found that employees are generally well trained regarding the existing information security threats, but when it comes to the SNSs, there seems to be an important gap, as the training content is not adapted to online realities. Indeed, it has already been found that in order to safeguard information against insider threats, organizations should employ SETA (security, education, training and awareness) programs (Molok, Nuha, Ahmad, & Chang, 2010). Moreover, 'security awareness' seems to be an important security risk factor when employees are using social media at work (Fagnot & Paquette, 2012). Our research confirms previous findings and extends them by highlighting the need for more efficient training and educational programs that need to consider online realities (challenges, practical insights, evolving security risks, etc…)

Interestingly, SNSs do not seem to be correctly approached in existing organizational information security policies. Past research (Hekkala et al., 2012) confirmed the need to establish an appropriate policy. In that context, our research concludes that online authentication and identification needs to be better handled in existing information security policies in order to warn employees not to 'trust' the online 'friend requests' without any verification. Our research also extends previous findings by confirming that SNSs have become an important security hole for organizations. What is even more worrying is that this is an external security hole that organizations struggle to effectively and efficiently control and monitor. Indeed, as the number of SNS sites continues to increase, especially in the mobile ecosystem, the threat to information security will further grow.

Implications for practice

Our study has some practical implications, given the importance of SNSs, growing challenges, and current growth and evolution of the SNSs in the mobile world. We suggest that this is the time for organizations to create a new organizational function that would act as a gatekeeper for all information flow related to SNSs. Moreover, our study shows that organizations should carefully evaluate different

threats, but also the benefits from SNSs and take these aspects into consideration when leveraging their information security policy.
Furthermore, the “liking” influence technique has a particularly strong effect in the SNS context, as employees tend to more easily accept phishing messages and acknowledge them as valid ones. This suggests that training and security awareness programs should highlight this influence technique as being particularly dangerous. In other words, more appropriate training and education programs should be designed that incorporate defenses against this type of influence.
Finally, our research suggests that, despite the fact that organizations need to leverage their existing countermeasures and adapt them more to SNS realities, employees seem to be more relaxed and less careful when it comes to detecting potentially suspicious social engineering activities.

Theoretical contributions
Future research on deception theory could use the results of our study to incorporate credibility, persuasion and motivation theories as useful theoretical support, which in our case provided a solid explanation for the phishing attacks’ effectiveness in the SNS context. In particular, the “liking” influence technique was found to be particularly effective and influential. This highlights the importance of Cialdini and James (2009), work which we situated in the particular context of SNSs. Moreover, we demonstrated that cognitive processing, influence, and motivation are very much facilitated in the context where email as a phishing method is not used. Instead of email being a communication channel, the SNS wall was used as a medium to attract potential victims. This not only highlights the risks behind this new method, but also demonstrates how that type of influence technique can have more serious implications if used in a different context.

Limitations and future research directions
Our study has some limitations, as we conducted our field experiment in only one organization, which might have influenced some of the insights gained from the interviewees. Moreover, the organization we studied is in the financial services industry. For future research, it would be good to extend the single organization context to more organizations and further test our results through a quantitative study where organizations from different industries are represented.
Furthermore, for the field experiment, we used one influence technique – liking, and it would be very interesting to understand how other influence techniques perform in the business context. Hence, future research could more deeply investigate how different influence techniques suggested by Cialdini and James (2009) (e.g. reciprocity, social proof, consistency, authority, and scarcity) could affect employee behavior.
Another limiting factor is that we did not capture any individual employee factors, such as security awareness, Internet proficiency, or specific demographics. While it would be very beneficial to have this background information, we did not proceed with this step for privacy reasons.

II. CONCLUSION

By synthesizing credibility, persuasion and motivation theories and combining two different research methods (field experiment and interviews), our research aimed to clarify phishing attacks’ effectiveness in the SNS context where the influence technique of liking is used. We also sought to understand how firms are dealing with the underlying threats. More precisely, we suggest that existing organizational SNS policies and procedures are not adequate and should be adapted to SNS realities where stronger employee identification and authentication is needed in combination with updated, clearer and more robust information security policies related to SNSs. A better understanding of phishing attacks by employees is still needed in a context where there is an existing disconnection between the SNS realities and the counter-measures that exist in organizations. We also argue that due to single sign-on applications that allow users to interact with other websites through their SNS credentials, the security risk is accompanied by a ‘multiplication’ effect, where compromising one credential can lead to multiple sites being compromised. Finally, insights from this study can help organizations to understand employees’ vulnerabilities to phishing attacks, which can serve as a basis for better security awareness and training programs.

REFERENCES

References

Abbasi, A., Zhang, Z., Zimbra, D., Chen, H., & Nunamaker, J. F., Jr. (2010). DETECTING FAKE WEBSITES: THE CONTRIBUTION OF STATISTICAL LEARNING THEORY. *Mis Quarterly, 34*(3), 435-461.

Al Zamal, F., Liu, W., & Ruths, D. (2012). Homophily and Latent Attribute Inference: Inferring Latent Attributes of Twitter Users from Neighbors. *ICWSM, 270*.

Algarni, A., Xu, Y., & Chan, T. (2015). Susceptibility to social engineering in social networking sites: The case of Facebook.

Algarni, A., Xu, Y., Chan, T., & Tian, Y.-C. (2014). *Social engineering in social networking sites: how good becomes evil.* Paper presented at the Proceedings of The 18th Pacific Asia Conference on Information Systems (PACIS 2014).

Alowibdi, J. S., Buy, U. A., Yu, P. S., & Stenneth, L. (2014). *Detecting deception in online social networks.* Paper presented at the Advances in Social Networks Analysis and Mining (ASONAM), 2014 IEEE/ACM International Conference on.

Baker, W., Hutton, A., Hylender, C. D., Pamula, J., Porter, C., & Spitler, M. (2011). 2011 data breach investigations report. *Verizon RISK Team, Available: www. verizonbusiness. com/resources/reports/rp_databreach-investigations-report-2011_en_xg. pdf*, 1-72.

Blakley, B., McDermott, E., & Geer, D. (2001). *Information security is information risk management.* Paper presented at the Proceedings of the 2001 workshop on New security paradigms.

Boyd, D., & Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship in Journal of Computer-Mediated Communication, 13 (1), article 11.

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication theory, 6*(3), 203-242.

Carlson, J. R., & George, J. F. (2004). Media appropriateness in the conduct and discovery of deceptive communication: The relative influence of richness and synchronicity. *Group Decision and Negotiation, 13*(2), 191-210.

Castillo, C., Mendoza, M., & Poblete, B. (2011). *Information credibility on twitter.* Paper presented at the Proceedings of the 20th international conference on World wide web.

Chitrey, A., Singh, D., & Singh, V. (2012). A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model. *International Journal of Information and Network Security (IJINS), 1*(2), 45-53.

Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2012). Detecting Automation of Twitter Accounts: Are You a Human, Bot, or Cyborg? *Ieee Transactions on Dependable and Secure Computing, 9*(6), 811-824. doi: 10.1109/tdsc.2012.75

Cialdini, R. B., & James, L. (2009). *Influence: Science and practice* (Vol. 4): Pearson education Boston, MA.

Cohen, D. (2013). Online fraud report. In N. Y. EMC, December 2013, p. 5. (Ed.).

Conti, G., & Sobiesk, E. (2010). *Malicious interface design: exploiting the user.* Paper presented at the Proceedings of the 19th international conference on World wide web.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*(1), 83-108.

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). *Why phishing works.* Paper presented at the Proceedings of the SIGCHI conference on Human Factors in computing systems.

Donath, J. (2007). Signals in social supernets. *Journal of Computer-Mediated Communication, 13*(1), 231-251.

Dwyer, C., Hiltz, S., & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 Proceedings*, 339.

Egelman, S., Cranor, L. F., & Hong, J. (2008). *You've been warned: an empirical study of the effectiveness of web browser phishing warnings.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Eisend, M. (2006). Source credibility dimensions in marketing communication–A generalized solution. *Journal of Empirical Generalizations in Marketing, 10*(2), 1-33.

Fagnot, I., & Paquette, S. (2012). Organizational Information Security: The Impact of Employee Attitudes and Social Media Use.

Ferguson, A. J. (2005). Fostering e-mail security awareness: The West Point carronade. *EDUCASE Quarterly, 28*(1), 54-57.

Gragg, D. (2003). A multi-level defense against social engineering. *SANS Reading Room, March, 13*.

Grazioli, S. (2004). Where did they go wrong? An analysis of the failure of knowledgeable internet consumers to detect deception over the internet. *Group Decision and Negotiation, 13*(2), 149-172.

Grow, B., Epstein, K., & Tschang, C.-C. (2008). The new e-spionage threat. *Business Week, 10*, 2008.

Harris, E., Perlroth, N., Popper, N., & Stout, H. (2014). A sneaky path into Target customers' wallets.

Healey, J. (2013). China is a cyber victim, too.

Hekkala, R., Väyrynen, K., & Wiander, T. (2012). Information security challenges of social media for companies.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24*(1), 61-84.
Hesseldahl, A. (2011). Lockheed Martin confirms it came under attack.
Hogben, G. (2007). Security issues and recommendations for online social networks. *ENISA position paper, 1*, 1-36.
Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74-81.
Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM, 50*(10), 94-100.
Jakobsson, M. (2007). The human factor in phishing. *Privacy & Security of Consumer Information, 7*(1), 1-19.
Jakobsson, M., & Myers, S. (2006). *Phishing and countermeasures: understanding the increasing problem of electronic identity theft*: John Wiley & Sons.
Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS quarterly, 39*(1), 113-134.
Kaspersky. (2013). KASPERSKY SECURITY BULLETIN - SPAM EVOLUTION 2013.
Kuikka, M., & Äkkinen, M. (2011). Determining the challenges of organizational social media adoption and use.
Kvedar, D., Nettis, M., & Fulton, S. P. (2010). The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. *Journal of Computing Sciences in Colleges, 26*(2), 80-87.
Li, C. (2010). *Open leadership: how social technology can transform the way you lead*: John Wiley & Sons.
Light, B., McGrath, K., & Griffiths, M. (2008). More than just friends? Facebook, disclosive ethics and the morality of technology.
Lindsey, L. L. M., Dunbar, N. E., & Russell, J. C. (2011). Risky business or managed event? Perceptions of power and deception in the workplace. *Journal of Organizational Culture, Communications and Conflict, 15*(1), 55.
Liu, W., & Ruths, D. (2013). *What's in a Name? Using First Names as Features for Gender Inference in Twitter.* Paper presented at the AAAI Spring Symposium: Analyzing Microtext.
Luo, X., Burd, S., Li, W., Brody, R. G., Brizzee, W. B., & Cano, L. (2012). Flying under the radar: social engineering. *International Journal of Accounting & Information Management, 20*(4), 335-347.
Malik, H., & Malik, A. S. (2011). Towards identifying the challenges associated with emerging large scale social networks. *Procedia Computer Science, 5*, 458-465.
Marett, K., Biros, D. P., & Knode, M. L. (2004). Self-efficacy, training effectiveness, and deception detection: A longitudinal study of lie detection training *Intelligence and security informatics* (pp. 187-200): Springer.
Mitnick, K. D., & Simon, W. L. (2001). *The art of deception: Controlling the human element of security*: John Wiley & Sons.
Molok, A., Nuha, N., Ahmad, A., & Chang, S. (2010). Understanding the factors of information leakage through online social networking to safeguard organizational information. *ACIS 2010 Proceedings*.
Nagy, J., & Pecho, P. (2009). *Social networks security.* Paper presented at the Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on.
O'Keefe, D. J. (2002). *Persuasion: Theory and research* (Vol. 2): Sage.
Ong, T. H., Tan, C. P., Tan, Y. T., & Ting, C. (1999). *SNMS-Shadow Network Management System.* Paper presented at the Recent Advances in Intrusion Detection.
Parsons, K., McCormac, A., Butavicius, M., & Ferguson, L. (2010). Human factors and information security: individual, culture and security environment: DTIC Document.
Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes. *Computers & Security, 30*(6-7), 486-497. doi: 10.1016/j.cose.2011.05.002
Proofpoint research. (2014). Security Threats to the Social Infrastructure of the Fortune 100.
PwC. (2014a). The Global State of Information Security® Survey 2015 Retrieved February 2015, from http://www.pwc.com/gx/en/consulting-services/information-security-survey/key-findings.jhtml
PwC. (2014b). INFORMATION SECURITY BREACHES SURVEY 2014
Richardson, R. (2008). CSI computer crime and security survey. *Computer Security Institute, 1*, 1-30.
Rosenblum, D. (2007). What anyone can know - The privacy risks of social networking sites. *Ieee Security & Privacy, 5*(3), 40-49. doi: 10.1109/msp.2007.75
Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security, 26*(1), 56-62.
SANS. (2012). Risk Assessment of Social Media.
Silic, M. (2016). *Understanding Colour Impact on Warning Messages: Evidence from US and India.* Paper presented at the CHI'14 Extended Abstracts on Human Factors in Computing Systems.
Silic, M., Barlow, J., & Ormond, D. (2015). *Warning! A Comprehensive Model of the Effects of Digital Information Security Warning Messages*. Paper presented at the The 2015 Dewald Roode Workshop on Information Systems Security Research, IFIP, Dewald
Skeels, M. M., & Grudin, J. (2009). *When social networks cross boundaries: a case study of workplace use of facebook and linkedin.* Paper presented at the Proceedings of the ACM 2009 international conference on Supporting group work.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133. doi: 10.1016/j.cose.2004.07.001

Steyn, T., Kruger, H. A., & Drevin, L. (2007). Identity theft—Empirical evidence from a Phishing exercise *New Approaches for Security, Privacy and Trust in Complex Environments* (pp. 193-203): Springer.

Sundie, J. M., Cialdini, R. B., Griskevicius, V., & Kenrick, D. T. (2012). The world's (truly) oldest profession: Social influence in evolutionary perspective. *Social Influence, 7*(3), 134-153.

Szwedo, D. E., Mikami, A. Y., & Allen, J. P. (2011). Qualities of peer relations on social networking websites: predictions from negative mother–teen interactions. *Journal of Research on Adolescence, 21*(3), 595-607.

Vishwanath, A. (2014). Diffusion of deception in social media: Social contagion effects and its antecedents. *Information Systems Frontiers*, 1-15.

Vishwanath, A. (2015). Habitual Facebook use and its impact on getting deceived on social media. *Journal of Computer-Mediated Communication, 20*(1), 83-98.

Wang, J., Gupta, M., & Rao, H. R. (2015). Insider Threats in a Financial Institution: Analysis of Attack-Proneness of Information Systems Applications. *MIS quarterly, 39*(1), 91-112.

Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems, 18*(2), 101-105. doi: 10.1057/ejis.2009.12

Workman, M. (2008). A test of interventions for security threats from social engineering. *Information Management & Computer Security, 16*(5), 463-483. doi: http://dx.doi.org/10.1108/09685220810920549

Wright, R. T., Jensen, M. L., Thatcher, J. B., Dinger, M., & Marett, K. (2014). Research Note-Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance. *Information systems research, 25*(2), 385-400.

Wright, R. T., & Marett, K. (2010). The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems, 27*(1), 273-303. doi: 10.2753/mis0742-1222270111