Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2012 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

7-15-2012

A Typology Of Social Engineering Attacks – An Information Science Perspective

Koteswara Ivaturi
Department of Information Systems & Operations Management, The University of Auckland Business School, Auckland,
k.ivaturi@auckland.ac.nz

Lech Janczewski
Department of Information Systems & Operations Management, The University of Auckland Business School, Auckland,
lech@auckland.ac.nz

A TYPOLOGY OF SOCIAL ENGINEERING ATTACKS – AN INFORMATION SCIENCE PERSPECTIVE

Koteswara Ivaturi, Department of Information Systems & Operations Management, The University of Auckland Business School, Auckland, k.ivaturi@auckland.ac.nz

Lech Janczewski, Department of Information Systems & Operations Management, The University of Auckland Business School, Auckland, lech@auckland.ac.nz

Abstract

Hackers are increasingly exploiting the social movement on the Internet, which is responsible for domestication of the web and its associated technologies, by using novel methods of online social engineering. However, there is not enough support in the form of published research that can help us gain a holistic understanding of human vulnerabilities that are central to online social engineering attacks. This paper extends prior published classifications and presents a new typology of online social engineering methods that manifest during the various information seeking contexts that users engage while online. Concepts borrowed from the field of information science help us to build this typology that groups attack vectors with different human information seeking modes. The typology can be readily used as educational material to improve end user awareness about online social engineering. In addition, the typology can be used as a conceptual starting point for future empirical research on human vulnerabilities in different information seeking contexts which in turn can inform systems designers to design more effective solutions that can help mitigate the effects of such attacks.

Keywords: Home internet users, Online social engineering, Human information seeking, Typology

1 INTRODUCTION

While talking about information security it is very common to think about threats that can be contained with the help of technical countermeasures such as email filters, network firewalls, anti- viruses etc., albeit there is a more subtle form of threat to which there is no direct solution. Many organizations are learning the fact that technical countermeasures alone cannot provide the required security as 'social engineering' provides a means to bypass them (Rhodes 2001). Social engineering allows attackers to psychologically manipulate their victims to change their behavior to divulge important sensitive information (Townsend 2010). Unlike other security vulnerabilities that are inherent to manmade software & hardware systems a key aspect of gaining insight into the nature of social engineering attacks involves a significant understanding of how the humans interact. The fact that not all humans are unique adds an additional layer of difficulty to understand this esoteric attack methodology.

The advent of the Internet and our increasing dependency on it has expanded the threat landscape of these attacks. According to a recent report released by Symantec in 2010, 65% of the world's online population has fallen victim to cybercrimes including computer viruses, credit card fraud and identity theft (Merritt 2010). Advances in technology that try to mitigate the effect of these attacks can be best described as 'lacking' partly because of the reactive nature of their detection mechanisms and partly because of the irresponsibility or ignorance on part of the user. The target demographic for our research is the home based internet user, who in the recent years has become an important unit of analysis given the range of activities he engages with on the web and yet there hasn't been enough research to focus on his training and awareness. Although there are a few published empirical studies that have analyzed how people respond to social engineering attacks a majority of them have used phishing as their primary test bed for their research (Grazioli 2004; Jakobsson, Tsow et al. 2007; Workman 2007; Vishwanath, Herath et al. 2011). While there are many other vectors that can be categorized as online social engineering attacks, a question arises whether there is any other way to understand or explain human vulnerability holistically. In this paper we present a two dimensional typology which could be used to correlate aspects of human vulnerability with the efficiency of online social engineering attacks. We try to achieve this by looking at the issue from a human web information seeking perspective. As such, this study lies at the unique intersection of fields of information science and information security. Such a typology we hope would become a conceptual starting point to create scope for more in depth research that could lead to developing procedures and informing the current information systems development lifecycle to mitigate the damages caused by such attacks.

The rest of the paper proceeds as follows. Section 2 provides the background and motivation for the paper. Section 3 gives an overview of the different attack vectors that can be classified as online social engineering attacks. Section 4 gives a brief overview of the information seeking field and draws on the results of a specific model that has 3 different modes of information seeking. Section 5 then presents a two dimensional typology of social engineering attacks with respect to the different information seeking modes described in the earlier section. In section 6 we conclude by discussing the application of this new research direction and the opportunities that it presents for the field of information systems security field.

2 MOTIVATION & BACKGROUND

As organizations started tightening their defenses due to an increased focus on information security, home based internet-users became attractive targets to cyber-attacks. A majority of the home based internet-users are highly unlikely to be trained in internet protection and hence become highly vulnerable & easy targets to online hackers and scammers (Furnell, Bryant et al. 2007). Another reason is the domestication of the web in the recent years that has further fuelled the extension of the threat landscape into the internet-user's home. With increased adoption of internet based services both through broadband penetration at home and on mobile devices this home based internet-user population is only going to grow in the next few years (Furnell, Tsaganidi et al. 2008). Hence, it is important to understand the internet-users' ability to protect their personal information and computing resources from potential compromises. Despite the importance of this area the main focus of the behavioral information systems security research was carried out in the organizational context, trying to study the organization's employees' compliance with security policies and procedures (Vroom and von Solms 2004; Seppo, Mikko et al. 2007). While it is important to continue to conduct research in the organizational setting it is important not to ignore home based internet-user's security. In fact, it is the organizations that should have a vested interest in enhancing end-user security because a compromised internet-user's computer can be used as a bot in a network of compromised computers to launch attacks such as denial of service attacks on the organization (Furnell, Bryant et al. 2007).

Mitnick and Simon (2005) mention that it is often very hard to detect and almost impossible to defend against social engineering attacks (Mitnick and Simon 2005). Indeed, most of the literature reflects on the importance of internet-user's security awareness and training programs as the best possible way to mitigate the damage caused by these attacks. However, as mentioned before most of this research has concentrated on the internet-user's awareness in an organizational context and not on the internet-user at home. In a more recent study Kritzinger et al. (Kritzinger and von Solms 2010) argue that the number of information security awareness programs available for home based internet-users is far less in comparison to that for users in an organizational context. The few awareness programs that are available are online programs that are disparate and difficult to find for a novice user. One of the main differences that separate home users and non-home users is the fact that in an organizational setting, the users are forced to follow security policies laid out by the company and their actions are constantly monitored. Home users do not have any such enforcement and for a large part have to be self-monitoring and directing. In addition to this, the lack of proper training and knowledge will result in internet users' exhibiting unsafe computing behaviors such as browsing unsafe websites, downloading suspicious software, sharing passwords with friends and family and not protecting home wireless networks making it all the more conducive for a hacker to compromise their systems.

Another area that lacks enough research is the consideration of the human vulnerability in the design phase of information systems security. The focus of information systems design has definitely shifted from the traditional 'system centered' approach of the 1970s to the 'user centered' approach of the late 1980s (Newby 2001). Despite this change, although designers of information systems have been successful at including 'human factors' they haven't succeeded at integrating 'human behaviors' (Jin and Fine 1996). In another earlier study Rouse et al. state that the design methods were limited in their usefulness as a result of neglecting the human side in the design process and emphasized the use of context, different information seeking modes & various cognitive styles in design (Rouse and Rouse 1984). This lack of consideration of 'human behaviour' is what is clearly being exploited through attacks that employ social engineering principles that feed on human vulnerability. Typically, information systems are developed with adherence to the software development life cycle (SDLC) which is a general approach to the development of any information system. Although there are established studies addressing security component in the design of information systems (Baskerville 1993) in the fast moving world of 'launch & iterate' security has only become a liability than an asset. Based on the above arguments it is clear that there is a long way to go before we see elements of human behavior being considered as part of the design process of building an information system and hence there is a clear need for some research on the issue.

3 ONLINE SOCIAL ENGINEERING – DEFINITION & ATTACK VECTORS

The art of deception is central to the success of a social engineering attack. The art itself is not new and has been mastered to perfection way before the invention of technology. But the advent of the World Wide Web has further augmented the reach and potential of such attacks. Laribee defined the term “online social engineering” as a way of gaining passwords and usernames from people without their permission by targeting vulnerable computers online (Laribee. 2006). While that is accurate, the true potential of “online social engineering” has spread beyond the mere collection of user names & passwords to simple end goals like making the user click on a malicious link that will trigger the execution of a script which will then exploit the operating system or web application vulnerability. As such, the meaning of online social engineering is defined as the use of web in order to influence online user behaviour by exploiting the vulnerabilities in both humans & web applications individually or in unison. It is to be noted that although what happens after a victim clicks on a malicious link is very much like the traditional technical hacking, the initiation of the attack is through setting up a situation that lures the user into the trap. This is where the distinction lies between traditional technical security attacks and online social engineering. A taxonomy is always useful to gain a better understanding of any phenomenon and to build accurate measures that cater to it. A good taxonomy that is mutually exclusive, unambiguous, comprehensive and comprehensible can further explain this distinction (Lindqvist and Jonsson 1997). Laribee in her thesis suggests taxonomy to classify these attacks based on three broad criteria ‘close access techniques’, ‘online social engineering’ and ‘intelligence gathering’. However, the list of different attack vectors that especially fall under online social engineering wasn’t up-to-date while ‘information gathering’ is not strictly unique to social engineering. A recent study suggests a taxonomy that addresses the issues stated above to a fair extent. According to this taxonomy online social engineering entails attack vectors like phishing, malware that propagates itself through email, social network spam, search engine poisoning and pop-ups (Ivaturi and Janczewski 2011). The following sub sections discuss these vectors and extend it with a few more.

3.1 Phishing

Phishing is a fraudulent process of acquiring sensitive and personal information by masquerading as a trustworthy entity and is mostly carried out over email. Over the years this problem has not only grown in size but also in complexity (Lee, Choi et al. 2007). Typically, the attacker generates hundreds of random email addresses and sends a blanket email to all of them hoping that at least a small percentage of the potential victims will take the ‘bait’. The nature of the bait involves a realistic looking message with a fraudulent call-to-action and a website that the attacker uses to collect the victim’s information. This is a type of attack where the attacker is deceptively influencing the victim and persuading him to divulge sensitive information.

3.2 Money Laundering – Nigerian 419 scam

The 419 advance fee fraud scam is a money laundering attack mechanism that tries to convince a user to take part in some ‘too good to be true’ financial deal. Usually victim users are reached through email and through the content of the email they are convinced into performing an action that would leave them at a disadvantage (Glickman 2005). An example theme of such a scam includes victims being offered a part of a large sum of money that is stuck in some bank account of a very rich dead man. The sender then asks for your help to move that money into a legitimate bank account while offering a sizeable commission. But the sender also asks you to send your bank account details and some earnest money to facilitate the transfer. The social engineering angle lies in the pretext of the story behind the scam and the leverage of human traits like greed and curiosity to convince them to take part. Many other such scams with varying themes have emerged in the past few years while the central idea always remained the same.

3.3 Malware

This vector is probably the most effective and hence most successful of all types of social engineering attacks due to its pervasive and persistent nature. This attack vector is a combination of both psychological and technical ploys and usually feeds on unsuspecting average users, a number that runs in thousands (Abraham and Chengalur-Smith 2010). As the technology that thwarts malware has evolved so has the complexity of the malware attacks primarily due to the reason that the psychological tactics of the attackers have also evolved.

3.3.1 Malicious downloads

It is reported that by 2015 approximately 4.1 billion email accounts will be used as a form of communication (Radicati Group 2011) and hence remains the most important malware delivery vehicle for the attackers. The tactics used here to persuade the user to perform an action mentioned in the email could be by eliciting the victim's curiosity by using catchy and intriguing lines that make the victim open the email. The 'Lovebug' worm in 2000 is a great example of this, where the attacker's email had the subject line 'ILOVEYOU' and an attachment that looked like a text file which made the unsuspecting and curious open the attachment only to be infected with a script that sent a copy of itself to everyone in the address book on behalf of the victim. The use of 'Trojans' is often another often well-known attack method that uses social engineering principles in spreading malware. The guise is to manifest itself as an executable file of value but which on execution runs a script that overwrites system controls.

3.3.2 Malware through pop-ups

Pop-ups are random alerts messages that open in a new window and are usually used as means for online advertising. The attackers use this form of attack to present messages that elicit the victim's fear or greed quotient that will eventually persuade them to perform the intended call for action. Recent examples include the emergence of 'scareware' where pop-ups appear that contain a fake message stating that victim's computer has been detected with a virus and that the user has to download a particular anti-virus to remove it (FBI 2010). Typical users panic and download the software with the intent to fix their computer but in doing so inadvertently infect their system with malware carried in the software.

3.3.3 Search engine poisoning

Search engine poisoning (SEP) is a method used by attackers to lure people to his website by employing certain "black hat" or unethical techniques. When the unsuspecting user clicks on the search engine result, because he deems it to be relevant to his query, he is redirected to another website that tries to persuade the user to or automatically downloads malware. A typical attack of this form usually kick-starts when there is a significant global event. Tools like Google trends are used to monitor such phenomena and whenever a particular keyword is found to be trending, the attackers build fake websites seeded with malware and expose it to search engine crawlers (Townsend 2010). The social engineering angle for this form of an attack is in the fact that the attacker is exploiting the trust that users have in the search results provided by the search engines to launch the malware attack. SEP is becoming increasingly popular as it doesn't even need to elicit the human emotions required for a typical social engineering attack as it is already created through the occurrence of the global events.

3.4 Clickjacking

Clickjacking is a relatively recent attack vector that tricks an unassuming user to click on a malicious link while the intention of the user is to interact with a legitimate website of choice. A typical clickjacking scenario as described by Grossman and Hansen (Hansen and Grossman 2008) involves two websites – Target website T and malicious website M. The target website is something that is of high value to the attacker and these include the likes of mail clients, online banking, auction sites etc., The malicious website is something which is in the control of the attacker. The attacker then loads a targeted region of T like, placing a bid, creating a status message, clearing inbox etc., and places it in an invisible iframe on M. The user thinks he is clicking on a regular link on M but actually clicks on a link placed T which is juxtaposed with M and gets compromised. The social engineering angle here is in the lure that the user falls into by clicking the link placed in the malicious iframe. Clickjacking scams on Facebook and twitter in recent times have been found to use provoking labels like 'Don't click', NSFW (Not safe for work), 'Shocking scenes' on the malicious page buttons to incite users to click on these bad links. (Balduzzi, Egele et al. 2010)

3.5 Malvertising

Over the past decade significant investments have been made by companies like Google, Microsoft & Facebook to attract users to online advertisements. Malicious agents have taken advantage of this to attract users to malicious websites that serve malware. The Web 2.0 functionality has helped the cause by allowing third party users to share their content across different networks through widgets, frames and JavaScript banners. Malicious agents exploit the vulnerabilities in these widgets and frames to redirect users to malicious websites (Sood and Embody 2011). This attack method is called as Malvertising or malicious advertising and has been reported as one of the biggest malware delivery vehicles in the recent past (Bluecoat 2011). The social engineering angle is in the trust that user has in the online advertising model – for example it is common for a click on advertisement to re direct to another website and this trust makes malicious redirections seem less like a red flag. Also, when malicious advertisements appear on well-known websites the trust that users have on that website is exploited. For example there were reports of malvertisements on websites like the New York times, Facebook & the London stock exchange in the past (Vratonjic, Manshaei et al. 2011).

4 HUMAN INFORMATION SEEKING BEHAVIOUR

During the last decade the web has become the prime destination for an increasing number of users to find and disseminate information (Martzoukou 2005). Users have been using the web for all kinds of information seeking purposes. As the web moved from its original static and passive version of web 1.0 to the current dynamic and active version of web 2.0 it allowed the user to don a more active role in the whole web ecosystem. This made the study of the user behavior on the web extremely important to gain a richer understanding of the real utilization of the web as an information source.

The uses and gratifications theory (UG) which is founded on the assumption that audiences are active in their consumption of media content was used to study the different motivations of the consumer to use the web (Levy and Windahl 1984; Perse 1990). The UG theory was seen well suited to study the Web 2.0 environment as it provided scope for high levels of interaction through chatting, using search engines & social network sites etc., Some studies that were conducted under the purview of UG theory found that users use the web for both instrumental &

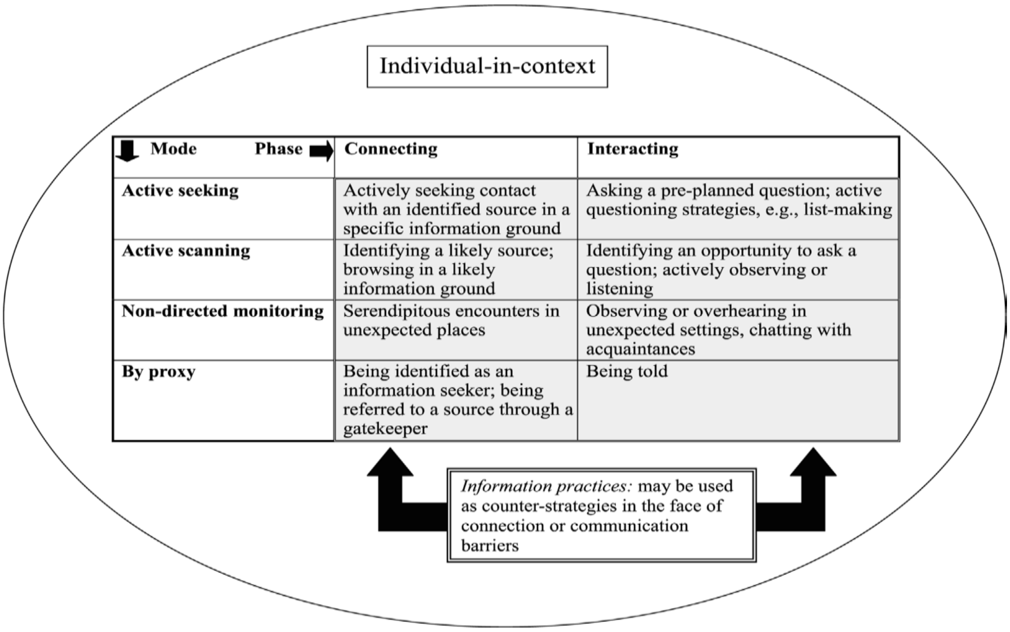
ritualistic reasons (M.Rubin 1994). Examples of instrumental reasons mentioned in the literature are monitoring current events and issues, searching for information to make decisions or accomplishing tasks while examples of ritualistic reasons are keeping in touch with friends through email and social networks or using the web for entertainment (Tewksbury and Althaus 2000). Although the UG theory provides a good foundation to understand the motivations of users to choose internet for personal gratifications, due to some of its fundamental assumptions it does not provide a holistic perspective of the actual web behavior. For example Katz & Blumler in their research mention that (Katz, Blumler et al. 1973) one of the assumptions of the UG theory is that audiences are always active in seeking for the media outlets for gratification purposes. While this is needed to explain the reason why users 'choose' a media outlet, it does not explain real user behavior after the media is chosen. For example, experiences like'browsing' which are known to be categorized as a passive online task is not catered to by the UG theory. Another assumption mentioned in the article was that media always compete with other more conventional and traditional sources of need & satisfaction. To study online behavior this assumption does not add any relevance or value as the premise to this study is that the web has become the numero uno source of information seeking & gratification over the past decade.

Information science on the other hand has evolved into forming strong associations with the fields of information systems, computer science & human computer interaction with design and development of information systems as its core concepts (Keshavarz 2008). The field of information science that deals with the phenomenon of human information seeking behavior is better suited to provide insights into user behavior on the web. The origin of this field is usually attributed to the Royal Society Scientific Information Conference in 1948 that was held due to the post World War II increase in the amount of scientific literature that wasn't published until then due to war time restrictions (Wilson 2000). Although initially the field had a focus on a 'system centric' approach addressing issues related to functionalities of information retrieval systems the focus shifted towards a 'person centered' approach since the early mid-1970s allowing other disciplines like psychology and sociology to inform concerns related to information processing and cognition (Wilson 2000). Several researchers like Wilson, Dervin, Ellis, and Kuhlthau were responsible for this change by publishing various human information behavior models during the mid-1980s. While organizational information seeking was the focus even in this field, Savolainen in 1995 developed the Everyday life information seeking model (ELIS) that focusses on a variety of domains in which information seeking occurs in our day- to-day lives (Savolainen 1995). The ELIS model provided a holistic framework to understand source preferences and use patterns of individuals' selection and application of the same to solve problems or to make sense of their everyday world issues. The value of ELIS over the previous models lies in the differences that as the other models try to explain the behavior of information seeking that starts with an uncertainty or knowledge gap the ELIS model starts with a sense of coherence and hence provides a holistic explanation of the phenomenon (Rieh 2004). Pamela Mckenzie, in her study of information practices of 19 Canadian pregnant women with twins, used the ELIS framework to develop a two- dimensional model that describes various modes of information practices (McKenzie 2003).

Drawing from the extent literature on information seeking McKenzie originally tends to investigate the characteristics of two modes, active and incidental or accidental information seeking but quickly identifies inadequacies that arise from her research data. These discrepancies eventually led her to come up with the following four modes of information practices that can be found be seen in Figure 1. The examples used to explain the four modes below are hypothetical but fit the descriptions given in the McKenzie model.

- **Active seeking**: In which users actively seek for information based on a preexisting need (a goal) and perform a systematic search. Ex: Going into a book store to find a specific book.

- **Active scanning**: In which the users have identified a particular source as a place they are likely to find useful information. They do not specifically have a particular goal in mind



Individual-in-context

Mode ⬇ Phase ➡	Connecting	Interacting
Active seeking	Actively seeking contact with an identified source in a specific information ground	Asking a pre-planned question; active questioning strategies, e.g., list-making
Active scanning	Identifying a likely source; browsing in a likely information ground	Identifying an opportunity to ask a question; actively observing or listening
Non-directed monitoring	Serendipitous encounters in unexpected places	Observing or overhearing in unexpected settings, chatting with acquaintances
By proxy	Being identified as an information seeker; being referred to a source through a gatekeeper	Being told

Information practices: may be used as counter-strategies in the face of connection or communication barriers

Figure 1. McKenzie's four modes of information seeking (McKenzie 2003)

while they look at these sources. Ex: Going into a book store without any specific book or title in mind.. Ex: Going into a book store without any specific book or title in mind.

- **Non-directed monitoring**: In which users serendipitously find information in an unlikely place or while scanning information sources that they use daily. Here, users do not have any goal in mind and their need triggers when they are exposed to information that they had no intention to look for. Ex: Finding a book that you like at a roadside vendor on your way to somewhere.

- **By proxy:** In which users find information through the initiation of another agent. Ex: Learning about a new book or title through a friend.

In the next section a typology of online social engineering attacks is presented by grouping each attack vector described in earlier section with specific information seeking modes as found in the McKenzie model. The 'By proxy' mode is not used as part of our typology because we are interested in analyzing individual human vulnerability and not the proxy state of it.

5 A TYPOLOGY OF SOCIAL ENGINEERING ATTACKS

In this section we present a typology of social engineering attacks based on the likelihood of exposure to these attacks for users engaged in each of the three information seeking modes – Active seeking, Active scanning and Non-directed monitoring.

5.1 Social engineering attacks in the context of active seeking

Wilson describes the act of active seeking of information as a behavior exhibited by individuals when they experience a lack of knowledge about a specific topic (Wilson 2000). This goal oriented behavior helps them to carry out a systematic and preplanned effort in order to the fill the knowledge gap. This effort will involve users formulating & executing planned item queries and repeating the query process until the goal of reducing the knowledge gap is fulfilled. Johnson and Meischke call this purposive information seeking and define it as "the purposive acquisition of information from selected information carriers" (Johnson and Meischke 1993). Another behavior that is relevant to the act of active information seeking is principle of least effort. According to this principle humans have a tendency to choose & use easily available information without consideration of the quality or reliability concerns (Bates 2002). This behavior makes people using search engines and other information retrieval systems vulnerable to manipulations especially if they are subtle to draw upon the various personal and environmental factors. In a recent study on deception related to Personal recommendation agents (PRA), Xiao & Benbasat study the effects of a deceptive PRA on users' choice of products and found that manipulations made on the recommendations can have a significant effect on user's choice to their detriment (Xiao 2007). Appropriately designed information systems like PRAs can effectively reduce the effort on the user in finding information quickly and readily, while improving their decision quality. Albeit, the degree to which the system actually helps the customer in the search process depends on the objective of the person who created the system (Hill, King et al. 1996). With the explosive growth of content on the web, search engines have become the number one source for information seeking on the web. The use of search engines on the web can be classified as an act of 'active' information seeking as after all the user doesn't randomly sit at a computer and start thinking of search queries (Rose and Levinson 2004). Searching is merely a means to an end and the need to use a search engine is triggered by an underlying goal, an information gap that the user is trying to bridge.

5.1.1 Mapping

Accordingly, we can classify search engine poisoning (SEP) described in section 3 as an attack vector that can directly affect users who are actively seeking information using search engines. Similarly, a malicious download in the form of a Trojan can be classified as an attack effecting active seeking users. Although the user might use a search engine to find a webpage to download a file, software package etc., the case of malicious downloads in the form of Trojans is different from SEP. While SEP leverages the concept of black hat Search Engine Optimization (SEO) a malicious download uses plain deceptive techniques to convince the user of its value on using it.

5.2 Social engineering attacks in the context of active scanning

The behavior of active information scanning is a form of regular or habitual information acquisition and is different from active information seeking where the behavior is ad hoc. Users who exhibit such a behavior usually place themselves in situations which improve the likelihood to find useful information. Examples of active scanning are cases where users revisit information sources that they've found useful in the past or a common place where they know that information is collated on a regular basis (McKenzie 2003). What is specific about this mode is that while users engage in this behavior they do not have any expectation to find anything specific (Vandenbosch and Huff 1997).There are references to this form of information seeking as being 'passive' & 'directed'- 'passive' because users do not have an active need to find anything specific and 'directed' because they place themselves in situations where they are likely to find useful information (Bates 2002). Other references describe this behavior as 'conditioned viewing' where users while actively scanning their information sources also differentiate between the different websites or pages that they expect to provide relevant information. This habitual differentiation leads to users returning to these websites to regularly browse or to keep abreast of new content through updates (Choo, Detlor et al. 1998). Based on the above arguments users that might engage in active scanning of information will most likely be users of email, social networks or just bookmarks to regularly scan for useful information. Users checking their email as a ritual do not have a specific goal in mind but are aware of the fact that they could find potentially useful information based on previous experience.

5.2.1 Mapping

Phishing that was discussed in section 2 as a social engineering attack can be categorized as an attack vector that can affect users involved in information scanning. Similarly, users browsing online social networks spend so much time because they want to keep in touch with what's happening with their friends and family. Again there is no specific goal in mind but the user of an online social network knows that there could be potentially useful information in the form of a status update from anyone in their network. Accordingly, clickjacking discussed in section 3 can also be categorized as a potential attack vector that can affect users involved in information scanning behaviors. Also, money laundering or the 419 scam can be slotted into this category as the primary vehicle to deliver the scam is through email which as discussed before is primarily used for information scanning.

5.3 Social engineering attacks in the context of non-directed monitoring

Non-directed monitoring is the behavior that involves a user accidently encountering a source of useful information in an unlikely place. The user usually is not aware of the need for information until he or she encounters it. This behavior corresponds to Wilson's passive attention (Wilson 1999), Choo et al.'s undirected viewing (Choo, Detlor et al. 1998), Ross's finding without seeking (Ross 1999). Usually, there are two situations that might emerge in such engagement. One of them is where users might find the information discovered as useful on the spot, this is where the information need and acquisition happens simultaneously. Although there is no prior cognizance of the information need it is triggered on encountering a specific piece of information. This could then lead the user to jump to another information source immediately or later in order to satisfy the need. The second situation is the one described by (Toms 2000) as the process of serendipitously recognizing the usefulness of information on encountering. Although subtle, there is a slight difference between serendipitous encountering and the former situation. The oxford dictionary defines serendipity as the occurrence and development of events by chance in a happy or beneficial way (Oxford 2012). Although there is a significant contribution of chance in inducing serendipity there is an element of preparation as well (Foster and Ford 2003). While discussing serendipity in information seeking Toms suggests that a person's prior knowledge together with the understanding of the value of the information usually influences the encounter of the information. This reflects the existence of a subconscious awareness for what he or she has set out to seek and will recognize it when encountered. For this paper we are considering both situations mentioned above as a single phenomenon as the common denominator between the two is that a priori, there is no intent to seeking information.

In this mode users usually scan large chunks of information from varied sources until something catches their attention. They quickly make a decision about the usefulness of the information that caught their attention and start the process again. Choo et al. describe this process as 'starting' and 'chaining' corresponding to the Ellis model of information seeking behaviors (Ellis 1989; Choo, Detlor et al. 1998). 'Starting' occurs when users begin their browsing behavior at preselected default homepages such as news or magazine sites. 'Chaining' occurs when viewers notice items of interest (often by chance) and follow links to gather more information on those items. In another related study, Barbara Kwasnik describes the actual physical activities associated with browsing and mentions that users do not scan the whole information horizon in a single movement but rather take a glimpse, look further at things that might interest them and then take another glimpse and so on (Kwasnik 1992).The Ellis model of information seeking describes a behavior called 'differentiating' that is relevant to studying human vulnerability. Differentiating is the act of users filtering and selecting from among the sources that were used at the 'starting' phase based on differences between the nature and the quality of information offered .This act of selection is based on individual's prior experiences, peer recommendations or reviews from credible sources (Ellis 1989).

5.3.1 Mapping

Based on the arguments presented above and mapping them to the list of attacks discussed in the section 3 we categorize popups & malvertising as possible vectors for attacks in non-directed monitoring mode. Both attack vectors fit the description as the content that they deliver are often discovered as a result of some random browsing behavior.

6 SUMMARY & CONCLUSION

The objective of this paper is to primarily build a conceptual foundation for future empirical research on online social engineering. The table seen below as figure 2 summarizes our discussion and culminates into a two dimensional typology of social engineering attacks. One of these dimensions is drawn from the knowledge we have about current vectors that should be considered as online social engineering attacks. Typically, although phishing has been the attack vector that got the most attention from the academic fraternity we feel other vectors mentioned in this paper need to be studied in depth to gain a holistic understanding of the current online social engineering threat landscape. From a practitioner standpoint, there is an urgent need to start integrating information about these new vectors into current security programs to help spread the awareness, especially amongst home based internet users. A recent paper that studied the adequacy of security policies for online banking reiterates the point discussed earlier that there is significant focus on educating users about phishing, which is good, while lacking significantly on creating awareness on the other vectors (Ivaturi and Janczewski 2011).

The other dimension of the typology groups the same attack vectors with different information seeking modes of the users on the web. The grouping is based on user behavior in each of the three modes and as a result the likelihood of being exposed to the attack vectors. This new dimension we hope will open a new avenue to conduct future research on online social engineering. For example as part of future research plans and an effort to validate the use of the typology, the authors of this paper are in the process of collecting research data as part lab based experimental study. The experiment involves randomly assigned users performing certain tasks that simulate the experience of engaging in each of the three information seeking modes. The experiment's objective is to test the variance in human vulnerability to online social engineering attacks that manifest in various information seeking modes. As such, the tasks that the users will perform will be induced with certain manipulations to mirror some of the attack vectors that were discussed as part of the typology. The experiment will collect data both objectively – from user

	Active seeking	**Active scanning**	**Non-directed monitoring**
Phishing		**X**	
Search Engine Poisoning	**X**		
Clickjacking		**X**	
Malvertising			**X**
Malicious downloads	**X**	**X**	
Popups			**X**
Money Laundering		**X**	

Table 1. A typology of social engineering attacks based on the users' information seeking modes

clicks and subjectively – as part of a research instrument. The results of such a study, we hope, can inform not only the current training and awareness programs on online social engineering but also the systems design fraternity by giving cues to new heuristics. The results of such a study we hope, can inform not only the current training and awareness programs on online social engineering but also the systems design fraternity by giving cues to new heuristics.

REFERENCES

Abraham, S. and I. Chengalur-Smith (2010). "An overview of social engineering malware: Trends, tactics, and implications." Technology in Society **32**(3): 183-196.

Balduzzi, M., M. Egele, et al. (2010). A solution for the automated detection of clickjacking attacks. Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. Beijing, China, ACM**:** 135-144.

Baskerville, R. (1993). "Information systems security design methods: implications for information systems development." ACM Comput. Surv. **25**(4): 375-414.

Bates, M. J. (2002). "TOWARD AN INTEGRATED MODEL OF INFORMATION SEEKING AND SEARCHING." New Review of Information Behaviour Research **3**: 1-15.

Bluecoat. (2011). "2011 Mid-Year Security Report." Retrieved 05/03/2012, from www.bluecoat.com/doc/16622.

Choo, C., B. Detlor, et al. (1998). A Behavioral Model of Information Seeking on the Web - Preliminary Results of a Study of How Managers and IT Specialists Use the Web. Proceedings of the 61st Annual Meeting of the American Society of Information Science, Pittsburgh, PA.

Ellis, D. (1989). "A behavioural model for information retrieval system design." J. Inf. Sci. **15**(4-5): 237-248.

FBI. (2010). "Protect Your Computer: Don‟t be Scared by 'Scareware'." Retrieved 02/03/2012, from http://www.fbi.gov/news/stories/2010/july/scareware.

Foster, A. and N. Ford (2003). "Serendipity and information seeking: an empirical study." Journal of Documentation **59**(3): 321-340.

Furnell, S., V. Tsaganidi, et al. (2008). "Security beliefs and barriers for novice Internet users." Computers &amp; Security **27**(7–8): 235-240.

Furnell, S. M., P. Bryant, et al. (2007). "Assessing the security perceptions of personal Internet users." Computers &amp; Security **26**(5): 410-417.

Glickman, H. (2005). "The Nigerian "419" Advance Fee Scams: Prank or Peril?" Canadian Journal of African Studies / Revue Canadienne des Études Africaines **39**(3): 460-489.

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.

Hansen, R. and J. Grossman. (2008). "Clickjacking." SecTheory Retrieved 05/03/2012, from http://www.sectheory.com/clickjacking.htm.

Hill, D. J., M. F. King, et al. (1996). "The perceived utility of information presented via electronic decision aids: A consumer perspective." Journal of Consumer Policy **19**(2): 137-166.

Ivaturi, K. and L. Janczewski (2011). A cross geographic content analysis of social engineering security policies for online banking. International conference on Informations technology, Systems & Management, IIM Kozikhode.

Ivaturi, K. and L. Janczewski (2011). A Taxonomy for Social Engineering attacks. CONF-IRM 2011 PROCEEDINGS.

Jakobsson, M., A. Tsow, et al. (2007). What instills trust? a qualitative study of phishing. Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security. Scarborough, Trinidad and Tobago, Springer-Verlag**:** 356-361.

Jin, Z. and S. Fine (1996). "The effect of human behavior on the design of an information retrieval system interface." International Information Library Review **28**(3): 249-260.

Johnson, J. D. and H. Meischke (1993). "A Comprehensive Model of Cancer-Related Information Seeking Applied to Magazines." Human Communication Research **19**(3): 343-367.

Katz, E., J. G. Blumler, et al. (1973). "Uses and Gratifications Research." The Public Opinion Quarterly **37**(4): 509-523.

Kritzinger, E. and S. H. von Solms (2010). "Cyber security for home users: A new way of protection through awareness enforcement." Computers &amp; Security **29**(8): 840-847.

Kwasnik, B. H. (1992). A Descriptive Study of the Functional Components of Browsing. Proceedings of the IFIP TC2/WG2.7 Working Conference on Engineering for Human-Computer Interaction, North-Holland Publishing Co.**:** 191-203.

Laribee., L. (2006). Development of Methodical Social Engineering Taxonomy Project. NAVAL POSTGRADUATE SCHOOL. MONTEREY, CALIFORNIA.

Lee, D. H., K. H. Choi, et al. (2007). Intelligence report and the analysis against the phishing attack which uses a social engineering technique. Proceedings of the 2007 international conference on Computational science and Its applications - Volume Part II. Kuala Lumpur, Malaysia, Springer-Verlag**:** 185-194.

Levy, M. R. and S. Windahl (1984). "AUDIENCE ACTIVITY AND GRATIFICATIONS: A Conceptual Clarification and Exploration." Communication Research Reports **11**: 51-78.

Lindqvist, U. and E. Jonsson (1997). How to systematically classify computer security intrusions. Security and Privacy, 1997. Proceedings., 1997 IEEE Symposium on.

M.Rubin, A. (1994). Media Uses and Effects: A Uses-and-Gratifications Perspective. in Media Effects: Advances in Theory and Research, Jennings Bryant and Dolf Zillmann. Hillsdale. NJ, Lawrence Erlbaum Associates.

Martzoukou, K. (2005). "A review of Web information seeking research: considerations of method and foci of interest." Information Research **10**(2).

McKenzie, P. J. (2003). "A model of information practices in accounts of everyday-life information seeking." Journal of Documentation **59**(1): 19-40.

Merritt, M. (2010). "Norton's Cybercrime Report: The Human Impact." Retrieved 1/03/2012, 2012, from http://community.norton.com/t5/Ask-Marian/Norton-s-Cybercrime-Report-The-Human-Impact-Reveals-Global/ba-p/282432.

Mitnick, K. D. and W. L. Simon (2005). The art of intrusion. Chapter 10, Wiley Publishing, Inc.

Newby, G. B. (2001). "Cognitive space and information space." J. Am. Soc. Inf. Sci. Technol. **52**(12): 1026-1048.

Oxford. (2012). Retrieved 03/03/2012, from http://oxforddictionaries.com/definition/serendipity.

Perse (1990). "AUDIENCE SELECTIVITY AND INVOLVEMENT IN THE NEWER MEDIA ENVIRONMENT " Communication Research **17**(5): 675-697.

Radicati Group, I. (2011). "Email Statistics Report." Retrieved 02/03/2012, from http://www.radicati.com/wp/wp-content/uploads/2011/05/Email-Statistics-Report-2011-2015-Executive-Summary.pdf.

Rhodes, K. (2001). " Operations security awareness: the mind has no firewall." Computer Security Journal **COMPUTER SECURITY INSTITUTE**.

Rieh, S. Y. (2004). "On the Web at home: Information seeking and Web searching in the home environment." Journal of the American Society for Information Science and Technology **55**(8): 743-753.

Rose, D. E. and D. Levinson (2004). Understanding user goals in web search. WWW '04 Proceedings of the 13th international conference on World Wide Web, NY, USA.

Ross, C. S. (1999). "Finding without seeking: the information encounter in the context of reading for pleasure." Inf. Process. Manage. **35**(6): 783-799.

Rouse, W. B. and S. H. Rouse (1984). "Human information seeking and design of information systems." Information Processing &amp; Management **20**(1–2): 129-138.

Savolainen, R. (1995). "Everyday life information seeking: Approaching information seeking in the context of "way of life." Library Information Science Research **17**(3): 259-294.

Seppo, P., S. Mikko, et al. (2007). Employees' Behavior towards IS Security Policy Compliance. System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on.

Sood, A. K. and R. J. Enbody (2011). "Malvertising – exploiting web advertising." Computer Fraud &amp; Security **2011**(4): 11-16.

Tewksbury, D. and S. Althaus (2000). "An Examination of Motivations for Using the World Wide Web." Communication Research Reports **17**(2).

Toms, E. G. (2000). Serendipitous information retrieval. Proceedings of the 1st DELOS Network of Excellence Workshop on Information Seeking, Searching, and Querying in Digital Libraries,, Zurich.

Townsend, K. (2010). "The art of social engineering." Infosecurity, **7**: 32-35.

Vandenbosch, B. and S. L. Huff (1997). "Searching and Scanning: How Executives Obtain Information from Executive Information Systems." MIS Quarterly **21**(1): 81-107.

Vishwanath, A., T. Herath, et al. (2011). "Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model." Decis. Support Syst. **51**(3): 576-586.

Vratonjic, N., M. H. Manshaei, et al. (2011). "Online Advertising Fraud." Retrieved 05/03/2012, from infoscience.epfl.ch/record/165674/files/OnlineAdFraud.pdf.

Vroom, C. and R. von Solms (2004). "Towards information security behavioural compliance." Computers &amp; Security **23**(3): 191-198.

Wilson, T. D. (1999). "Models in information behaviour research." Journal of Documentation **55**(3): 249-270.

Wilson, T. D. (2000). "Human Information Behavior." Informing Science **3**(2).

Workman, M. (2007). "Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security." Journal of the American Society for Information Science and Technology **59**(4): 662-674.

Xiao, B. a. B., Izak. (2007). "E-Commerce Product Recommendation Agents: Use, Characteristics, and Impact." MIS Quarterly **31**(1).