A Study of Email Deception Based on Situation Awareness Theory

Indicate Submission Type: Research-in-Progress

Hsieh-Hong Huang **Hsiao-Ting Tseng**

Chia-Lun Lo

Abstract

Information security-related research is traditionally focused on technical aspects, while little attention is paid to user behavior and organizational management and employee behavior is often neglected. In many cases, employees intend to comply with policies, but they cannot avoid "unintentional" violation of information security policies, that is, they are unaware of the existence of deception. Even if the user's intention to comply with the security policy is high and the behavior is toward compliance, it is still possible to have an information security violation in the case of "unawareness" or "mistrust," resulting in organizational losses. This study uses situation awareness theory to explore how email social engineering attacks can deceive users either unconsciously or unintentionally and to explore using current and possible training methods to reduce the possibility of employees falling victim to a successful email engineering attack.

Keywords: Social engineering, situation awareness theory, email deception, email fraud

Introduction

With the thriving and progressing of information technology and the Internet, information technology affects enterprise organizations by playing a particularly important role in their development. Information is an asset to an organization and has value like other important operating assets; thus, it should be properly protected. The purpose of information security is to protect information from threats, ensure continuous operations, minimize operational losses, and maximize return on investment and business opportunities.

Many organizations have spent a great deal of funds and resources on establishing various information and network security mechanisms to prevent, protect, and monitor the security of the information systems within the organization. However, although many security mechanisms are established, they often fail to prevent the employees from intentional or unintentional violation of organizational information security, namely, a violation due to desire for convenience, desire for increased production, curious peeking, or vandalism, making the carefully established security technology vulnerable (Greene and D'Arcy, 2010).

This study proposes that situation awareness (SA) theory can be used to explore the cognitive process of deception events in the scenario of low interactivity and to reveal how email social engineering attacks deceive subjects unconsciously or unintentionally. Further, it is proposed that individual-oriented training and attention should be implemented to improve the effectiveness of deception detection.

Theoretical Background

Theory of deception

Deception refers to an intentional manipulation of the environment by a fraudster in an attempt to trigger the deception targets to misunderstand environmental information. Johnson et al. put forward the theory of deception (TOD) in 1992, proposing that decision-making and information processing involves the two processes of information capturing and information interpreting. However, an individual's information-capturing process is usually difficult, that is, the individual has to undergo cognitive integration and decision-making in the absence of complete information. Deliberate deception is a cognitive interaction process between two individuals with conflicting interests: the fraudster and the target. In this process, the fraudster manipulates the target's environment to induce the target to make an incorrect cognitive interpretation so as to achieve the desired deception result (Johnson et al., 1992, 2001). Johnson et al. (1992) classify the information operation strategies of fraudsters in two types: dissimulation and simulation. The purpose of dissimulation is to deliberately conceal the facts, whereas simulation is aimed at intentionally displaying the wrong information. To strengthen a deception target's miscognition, the two types of strategies may be used jointly. Furthermore, the strategies can be divided into the three methods of information deletion, information modification, and information addition—all aimed at enhancing the target's miscognition (Johnson et al., 1992).

Fraudsters conduct deceptions by taking advantage of humans' rational information processing to manipulate an information recipient's cognition, namely, by displaying seemingly reasonable information after fabrication, distortion, and concealment of the original, true information and stimulating the recipient's cognition to information misprocessing or information association. Individuals detect deception by noting and interpreting the anomalies of targets in the environment, that is, deception detection occurs when individuals notice inconsistencies between their current experience and their past experiences (Grazioli, 2004).

Buller and Burgoon (1996) proposed interpersonal deception theory in 1996, defining deception as a deliberate conveyance of ideas or decisions that are likely to be inconsistent with reality. They tried to explain how individuals deal with real (or perceptual) deception on a conscious or subconscious level in face-to-face communication. When communicating with others, people often deceive or lie for some reasons, such as vanity, self-image maintenance, self-protection, credibility promotion, reduction of mutual conflicts, or evasion of punishment. Fraudsters create messages of false meaning in an attempt to make the deception targets believe that the messages are true and accept them as beliefs.

When only the communicator knows the truth, he or she controls the facts contained in the message to the receiver, whereas the recipient falls victim to deception or suspects the communicator of deception, as there is not enough evidence for the recipient to verify the communicator's statements or to infer whether the communicator's actions are legitimate. If communication is not static but influenced by the interaction between the individual and the target, the sender's deceptive (or covert) communication is affected by the recipient's deceptive and covert communication, and vice versa. Deliberate deception requires greater cognitive effort than needed by real communication, regardless of whether the sender attempts to falsify (lie about), conceal (omit) the facts, or behave in an ambiguous manner (Buller and Burgoon, 1996).

Before the prevalence of the Internet, deception was mostly attempted via interpersonal contact. With the development of Internet technology, deception attempts are quickly and openly delivered through the Internet. This, when combined with the anonymity characteristic of the Internet, promotes the

occurrence of Internet deception. Grazioli (2004) further explores why Internet users are less likely to detect Internet deception from the perspective of the information handling process for deception detection.

Social Engineering

Social engineering uses human weaknesses or relationships of interpersonal trust to gain information by influencing or persuading individuals. It often takes advantage of interaction with people to obtain account numbers, passwords, credit card passwords, ID numbers, names, addresses or other verifiable identity or confidential information. It uses fraudulent methods to obtain personal privacy information or organizational confidential information, or it induces the perception target to perform certain transactions or actions so as to obtain improper benefits. Humans tend to trust each other and easily expose personal information, which makes users vulnerable to social engineering attacks (Junger et al., 2017). Email social engineering attacks usually come in several forms: fraudsters pretending to be a sender, using business-related or interesting email content, and sending attachments or links that contain malicious programs. These attacks do not require the fraudsters to have computer expertise, as they can bypass the security protection layers that have been established with a huge cost as long as the employees fail to take precautions or lack sufficient awareness.

With the development of communication technology, deception behavior has evolved from the original “face-to-face” form to the use of “non-face-to-face” communication channels, such as telephone, email, web sites, and the Internet in general. In particular, email has the lowest level of media richness (Daft and Lengel, 1986) and its low level of interaction makes the recipient less likely to suspect or verify its authenticity.

The risk of falling victim to cybercrime may affect users' willingness to take risks in various online environments. It is necessary to take training measures to improve users' threat cognition and provide them with knowledge on how to reduce risks, as users' information security knowledge will positively affect their intent and inclination to adopt and use Internet security solutions. However, email social engineering has been constantly evolving, becoming increasingly complex and more attractive each year. It has even evolved into the form of Advanced Persistent Threat (APT), which is extensive in scale and deep in structure, with an ability to impose a threat in a continuous and multi-faceted manner. This makes it very difficult to defend against, and, as a result, the traditional method of using training to promote users' threat cognition has limited effectiveness.

Training

Traditional training involves a training strategy that creates the appropriate behaviors in specific situations and conveys expectations to the target learners through demonstration and practice (Jensen et al., 2017). These usually include a number of training methods, such as describing phenomena, providing clues or rules to identify phenomena, providing opportunities to practice the behavior, and participating in intensified training after practice. This training strategy is effective when used in a face-to-face and computer-based training environment and is more effective when used in combination with other training modes, such as self-learning or instructional teaching (Johnson and Marakas, 2000; Simon et al., 1996, Yi and Davis, 2001). People-oriented solutions often focus on: (1)employing training measures; (2)helping users make fine adjustments so as to achieve better decisions and create new designs or visual interfaces; (3)considering differences between individual decision-makers during a decision-making process (Nicholson et al., 2017).

In addition to the traditional method of shaping behaviors based on specific doctrines, Matthews et al. (2012) used an abstract behavior-shaping approach, namely, the Mindfulness approach, to instruct users to pause, think, and check email legitimacy. They found that the Mindfulness approach performs better than traditional rule-based education and training; specifically, abstract training is more effective than the rule-based approach in reducing the probability that the drill participant falls victim to the email social engineering deception. Further, they found that images are more effective than text when used in the training. This is (1)consistent with the conclusions of earlier studies that adopted cognitive adaptation theory to explain the difference in user performance between different

representation forms, such as tables, charts, and diagrams (Vessey, 1991; Vessey and Galletta, 1991), and (2)it is experimentally verified (Matthews et al., 2012). Training has been proven able to establish information security awareness in employees. However, to make employees willing to help maintain organizational information security, more measures are needed than information security technologies and policies alone. To this end, many scholars have begun to explore, from the behavioral aspect, how to make organizational information security policies effective (Bulgurcu et al., 2010; Hsu et al., 2015).

Regarding the learner's knowledge construction process, the constructivist Matthews (1994) believes that the establishment of knowledge comes from the interaction between the learner's own prior knowledge and the learning situation. Using a case related to the learner or using a lifestyle-based concept will cause learners' prior knowledge to have an impact on their learning in a specific situation. When using only information security-related knowledge and past cases as training materials, without connection to the learners' situation, the textbook will be a set of incomprehensible symbols for the learners. Then, the latter are unlikely to immerse themselves in the textbook situation (Matthews, 1994). Based on the above literature, the following hypotheses are proposed:

H1 : In the situation of email social engineering attacks, training has a significant impact on SA.

H2 : In the situation of email social engineering attacks, training has a significant impact on decision-making.

H3 : In the situation of email social engineering attacks, training has a significant impact on action performance.

Attention

Vishwanath et al. (2011) proposed an integrated information processing model based on information processing theory and interpersonal deception theory and used potential victims of email social engineering attacks as a sample to fine-tune and verify the model. They found that most individuals make decisions based on simple prompts in emails and that urgency cues in emails stimulate increased information processing, thereby short-circuiting the resources available for attending to other cues that could potentially help detect the deception. The study further distinguished between attention to the email's source, grammar and spelling, email title or subject line, and urgency cues, to investigate whether these four types of attention would have an impact on user response. It found that the impact is significant and direct—attention is negatively correlated to the possibility that a person responds to social engineering emails, with a higher degree of attention leading to a lower possibility of responding to deception emails (Vishwanath et al., 2011).

Attention is the first stage of information processing and indicates the amount of mental focus given to the specific elements of an event or object (Eveland et al. 2003), similarly to the concept of activation in TOD. That activation consists of allocating attention to cues based on the presence of discrepancies between what is observed and what is expected (Grazioli, 2004). When discovering that the expected ideal state differs from the one in the current situation, an individual experiences a need for cognition, with motivation, past experience, and environment all influencing this need. Individuals will use experience and prior knowledge as the first step in solving a problem and when the problem cannot be solved, information needs arise (Byström and Järvelin, 1995). When a received email is inconsistent with the existing state, source credibility becomes an important factor to consider, in addition to content credibility. Source credibility is defined as the extent to which the recipient of the message believes that the source of information is trustworthy and reliable (Petty et al., 1981; Sussman and Siegal 2003). In a previous study on an elaboration likelihood model, source credibility was classified into the peripheral route (Bhattacherjee and Sanford, 2006).

In a cognitive process, it is often necessary to process a great deal of information in parallel at the same time. However, attention resources are limited, especially in complex environments. In such environments, various information sources need attention and it is necessary to improve the prominence of the clues or use the target, working memory, and long-term memory to guide attention, which will help to mitigate the lack of attentional resources (Braune and Trollip, 1982). Based on the above literature, the following hypotheses are proposed:

H4 : In email social engineering attacks, attention has a significant impact on SA.
H5 : In email social engineering attacks, attention has a significant impact on decision-making.
H6 : In email social engineering attacks, attention has a significant impact on action performance.

Situation Awareness Theory

Situation awareness (SA) refers to a temporal and spatial perception of elements and events in an environment and an understanding of their representative meaning, as well as a perception of the change of their states when some variables change. SA includes understanding what is happening in the surrounding environment and understanding how information, events, and individual actions affect the original goal and purpose. A person with a strong SA usually has a higher level of knowledge about the input and output of the system and is capable of reasonably responding to situations, people, and events. As variables are controlled by decision-makers, people who lack or are weak in SA are often seen as the main cause of human error in an accident. Therefore SA is extremely important in the work environment, where information flow is extremely high and improper decision-making can lead to serious consequences. For decision-makers, SA is the key to understanding environmental conditions, especially in a complex and dynamic field (e.g., flights, air traffic control, ship navigation, power plant operation, military command) or in an emergency service field such as firefighting and policing (Endsley, 1995).

In a specific temporospatial environment, people perceive the environmental elements, generate SA, and further understand the meaning of these elements after perceiving them, and then use their understanding of these elements to predict the future state of these elements. The main purpose of SA is to enable decision-makers to recognize and understand the elements and their meanings in the environment at a specific time and in a specific space and to predict their future development so as to make appropriate decisions for action performance. SA can be applied to information security in threatening work environments. It makes it possible to perceive threatening activities and vulnerabilities in situations so as to actively protect data, information, knowledge, and intelligence. SA is achieved by developing and using solutions that can provide frequently-updated information and data from various sources, followed by applying knowledge and intelligence with technology and algorithms to identify behavioral patterns and detect potential and likely threats as well as true threats. For an operating team that deals with Internet security threats, SA—in the form of a system interface that is concentrated, rich, usually graphical, prioritized, and easy to search—exists within the organization or is related to the area of security responsibility. Moreover, user perception can be improved through collaborative methods (Mathews et al., 2012). Based on the above literature, the following hypotheses are proposed:

H7 : In the situation of email social engineering attacks, environmental status is significantly correlated with SA-related decision-making.
H8 : In the situation of email social engineering attacks, SA is significantly correlated with decision-making.
H9 : In the situation of email social engineering attacks, decision-making is significantly correlated with action performance.

Research Methodology

Research Framework

The research framework is based on SA theory and explores the factors that cause employees in an organization to “unintentionally” violate the security policy in a social engineering deception. The framework aims to understand how to reduce the information security incidents due to employees' "unawareness" or "mistrust" by providing of training and prompting attention focus, so as to avoid organizational losses. External system-oriented variables, such as system functions, interface design, load and stress, complexity, and automation are excluded from the study, whereas training is retained

as an individual-oriented variable. Moreover, following Vishwanath et al. (2011), attention is added as a new individual-oriented variable, as it has been confirmed that it has a significant impact on SA (Endsley, 2000).

In this study, two research methods will be adopted, namely, a field experiment and a questionnaire survey will be jointly conducted to complement the participation of research subjects in email social engineering drills. Experimental methods are suitable for exploring the causal relationship of events and a field experiment refers to conducting experiments in natural situations, as a real situation is better than a laboratory experiment method in terms of external validity, it is easier to generalize the results obtained in a real situation to other situations. The email social engineering drills are conducted by this organization and have been performed for many years. Therefore, there is no information security concern or ethical research concern.

Following to Churchill (1979), the study is conducted through several steps, in the following order: specifying the domain of the construct, generating a sample of items, collecting data, purifying measures, collecting data, assessing reliability, assessing validity, and developing norms.

Task and Measurements

This study is planned to be conducted in cooperation with the Eastern Coastal Patrol Office, Taiwan. It consists of designing a bait letter that conforms to the organization's operating situation in relation to email social engineering attacks. Further, it involves manipulating the sender's name, subject, and text to generate different situations, detecting action performance according to the indicator of whether the participants in the social engineering attack drills read the letter and open the attachment file. The final step is issuing post-test questionnaires.

To ensure the validity of the content, the research questions are taken from verified scales. Since the experiment will be conducted in Taiwan, the questions will be translated to Chinese. Moreover, the translation will be conducted by at least 3 professionals, followed by back-translation into English to ensure that the Chinese content is correct. Variables will be assessed by means of a Likert 7-point scale wherein scores range from 1 point (strongly disagree) to 7 points (strongly agree).

Pilot Test and Analysis

For small-scale testing, we will first conduct a pilot test on the first edition of the questionnaire and select a representative sample that is similar to the expected target of the questionnaire. This will be done to ensure that the experiment, questionnaire design, and the results are in line with expectations and to reduce the risk of research failure. Subsequently, we will perform reliability and validity testing to ensure that the design of the questions is correct. As regards reliability, Cronbach's alpha will be used to evaluate construct reliability. If the reliability value is lower than 0.5, the item-to-total correlation coefficient will be checked (Nunnally, 1994), with deletion of the items having a coefficient below 0.40.

As regards validity, this study will test content, construct, and discriminant validity relevant to the measurement questions. Content validity refers to the degree to which the scale's content is appropriate and to whether the questions capture the characteristics to be measured, as it is necessary to systematically test the appropriateness of the questionnaire (Churchill, 1979). In this study, the variable measurement items in the questionnaires are based on scales that have been empirically proven by relevant research. These items will be rigorously translated to improve content validity, and confirmatory factor analysis (CFA) will be employed to divide relevant variables into factor groups according to the factor loadings. The results of the analysis will be used to assess whether the research framework is consistent with the recovered data, so as to test the construct validity of the questionnaires and to examine the discriminatory validity of each construct.

In addition, participants will be asked whether they have encountered any problems during the process of answering the questionnaires, that is, any response and feedbacks from the participants regarding questions, sentences, semantics, and structures in the pilot test will be collected. These will be used as a reference for questionnaire revision.

Through pilot testing and modification, a formal version of the questionnaires will be generated for this study. To avoid non-response bias, a comparison will be performed between the early and the late stage of measurements. This will allow checking whether there is a significant difference in the number of employees and in the sex ratio (Armstrong and Overton 1977), so as to ensure external validity. Subsequently, a Cronbach's alpha reliability analysis and CFA will be carried out to evaluate the reliability and validity of the model measurements. As regards hypothesis testing, Structural Equation Modeling will be used to establish the structure model of the overall relationship, followed by testing each relational-structure hypothesis according to the data analysis results so as to verify the overall correlation structure.

Conclusion

The purpose of this study is to explore how email social engineering attacks result in individuals being deceived unconsciously or unintentionally and to explore current and possible training methods to reduce the likelihood of organization employees falling victim to such attacks. This study combines information security management, project management, organizational behavior, and other fields and uses a field experiment in conjunction with a questionnaire survey to complement email social engineering drills. The process is rigorous and the research contribution is high. It provides high research value and a contribution to the fields of information security management and cognitive process of deception.

This study is expected to provide the following contributions to academic research: (1)understanding the role of deception in social engineering, (2)understanding the factors affecting the intention of organization employees to read social engineering emails, (3)exploring the impact of SA on the action performance of identifying social engineering emails, (4)exploring the impact of training on SA and action performance in email social engineering, and (5)exploring the impact of attention on SA and action performance regarding email social engineering. To the practice, intensified training and prompts for attention focus can help to reduce the chances of successful email social engineering attacks. A theoretical basis is provided for using SA theory to explain the cognitive process of email social engineering.

Acknowledgements

This research was supported in part by the Ministry of Science and Technology of the Republic of China [Grant number MOST 108-2636-H-036 -001].

References

Armstrong, J.S. and Overton, T. S. 1977. “Estimating Nonresponse Bias in Mail Surveys,” *Journal of Marketing Research* (14:3), pp.396-402.

Bhattacherjee, A. and Sanford, C. 2006. “Influence Processes for Information Technology Acceptance: An Elaboration Likelihood Model,” *MIS Quarterly* (30:4), pp. 805-825.

Braune, R. J. and Trollip, S. R. 1982. “Towards an Internal Model in Pilot Training,” *Aviation, Space, and Environmental Medicine* (53:10), pp. 996-999.

Bulgurcu, B., Cavusoglu H., and Benbasat, I. 2010. “Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness,” *MIS Quarterly* (34:3), pp. 523-548.

Buller, D. B., and Burgoon, J. K. 1996. “Interpersonal Deception Theory,” *Communication Theory* (6:3), pp. 203-242.

Byström, K., and Järvelin, K. 1995. “Task Complexity Affects Information Seeking and Use,” *Information Processing and Management* (31:2), pp. 191-213.

Churchill, G. A. Jr. 1979. “A Paradigm for Developing Better Measures of Marketing Constructs,” *Journal of Marketing Research* (16:1), pp. 64-73.

Daft R. L., and Lengel, R. H. 1986. “Organizational Information Requirements, Media Richness and Structural Design,” *Management Science* (32:5), pp. 554-571.

Endsley, M. R. 1995. "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors* (37:1), pp. 32-64.

Eveland, W. P. Jr., Shah, D. V., and Kwak, N. 2003. "Assessing Causality in the Cognitive Mediation Model A Panel Study of Motivations, Information Processing, and Learning During Campaign 2000," *Communication Research* (30:4), pp. 359-386.

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), pp. 149-172.

Greene, G. and D'Arcy, J. 2010. "Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance," *Proceedings of the 5th Annual Symposium on Information Assurance*, pp. 42-49.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., Lowry, P. B. 2015. "The Role of Extra-role Behaviors and Social Controls in Information Security Policy Effectiveness," *Information Systems Research* (26:2), pp. 282-300.

Jensen, M. L., Dinger, M., Wright, R. T., and Thatcher, J. B. 2017. "Training to Mitigate Phishing Attacks Using Mindfulness Techniques," *Journal of Management Information Systems* (34:2), pp. 597-626.

Johnson, P. E., Grazioli, S., and Jamal, K. 1993. "Fraud detection: Intentionality and deception in cognition," *Accounting, Organization and Society* (18:5), pp. 467-488.

Johnson, P. E., Grazioli, S., Jamal, K., and Berryman, R. G. 2001. "Detecting Deception: Adversarial Problem Solving in a Low Base Rate World," *Cognitive Science* (25:3), pp. 355-392.

Johnson, P. E., Grazioli, S., Jamal, K., and Zualkernan, I. A. 1992. "Success and Failure in Expert Reasoning," *Journal of Organizational Behavior and Human Decision Processes* (53:2), pp. 173-203.

Johnson, R. D., and Marakas, G. M. 2000. "The Role of Behavioral Modeling in Computer Skills Acquisition: Toward Refinement of the Model," *Information Systems Research* (11:4), pp. 402-417.

Junger, M., Montoya, L., and Overink, F.-J. 2017. "Priming and Warnings are not Effective to Prevent Social Engineering Attacks," *Computers in Human Behavior* (66:1), pp. 75-87.

Matthews, M. R. 1994. "Constructivism and Science Education," in *Science Teaching,* Matthews M. (ed.), London: Routledge, pp. 137-161.

Mathews, M. L., Halvorsen, P., Joshi, A., and Finin, T. 2012. "A Collaborative Approach to Situational Awareness for Cyber Security," *Proceedings of the 8th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pp. 14-17.

Nicholson, J., Coventry, L., and Briggs, P. 2017. "Can we Fight Social Engineering Attacks by social means? Assessing Social Salience as a Means to Improve Phish Detection," *Proceedings of the Thirteenth Symposium on Usable Privacy and Security*, pp. 285-298.

Nunnally, J. C., and Bernstein, I. H. 1994. *Psychometric Theory*, New York: McGraw-Hill.

Petty, R. E., Cacioppo, J. T., and Goldman, R. 1981. "Personal Involvement as a Determinant of Argument-Based Persuasion," *Journal of Personality and Social Psychology* (41:5), pp. 847-855.

Simon, S. J., Grover, V., Teng, J. T. C., and Whitcomb, K. 1996. "The Relationship of Information System Training Methods and Cognitive Ability to End-User Satisfaction, Comprehension, and Skill Transfer: A Longitudinal Field Study," *Information Systems Research* (7:4), pp. 466-490.

Vessey, I. 1991. "Cognitive Fit: A Theory-Based Analysis of the Graphs Versus Tables Literature," *Decision Sciences* (22:2), pp.219-240.

Vessey, I. and Galletta, D. 1991. "Cognitive Fit: An Empirical Study of Information Acquisition," *Information Systems Research* (2:1), pp. 63-84.

Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. R. 2011. "Why do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model," *Decision Support Systems* (51:3), pp. 576-586.Watts Sussman, S., and Schneier Siegal, W. 2003. "Informational Influence in Organizations: An Integrated Approach to Knowledge Adoption," *Information Systems Research* (14:1), pp. 47-65.

Yi, M. Y., and Davis, F. D. 2001. "Improving Computer Training Effectiveness for Decision Technologies: Behavior Modeling and Retention Enhancement," *Decision Sciences* (32:3), pp. 521-544.