FACTORS INFLUENCING EMPLOYEES' SUSCEPTIBILITY TO PHISHING EMAILS: THE ROLE OF EMOTIONS

LeFranc, Nicolas, IESEG School of Management, Paris, France, nicolas.lefranc@ieseg.fr

Savoli, Azadeh, IESEG School of Management, Paris, France, a.savoli@ieseg.fr

Research-in-Progress

Abstract

Phishing is a deception method to gain sensitive information from an intended victim by using e-mails and web pages that appear to be from genuine people and businesses. To develop effective programs to fight phishing, researchers have adopted behavioural approaches to understand recipients' motivations, and beliefs in phishing detection. Past research shows that emotions play an important role in people's decision making process. Therefore, in the present study, we investigate factors influencing employees' phishing susceptibility from an emotion perspective. We argue that employees' emotional attachment to their organization, their normative commitment to the organization, and their perception of the urgency of the email can evoke positive and negative emotions in them, which in turn can influence their susceptibility to phishing attacks.

Keywords: phishing, contentment, anxiety, emotional attachment, normative commitment

1 Introduction

Phishing is a deception method to gain sensitive information from an intended victim by using e-mails and web pages that appear to be from genuine people and businesses. These messages usually encourage the potential victim to perform some actions. For example, they might request recipients to provide sensitive information, do an online transaction, login to a fake website, or download a malware (Jensen et al. 2017). Phishing attacks usually exploit the individual's cognitive biases and motivate them to rely on their heuristics behaviors. Phishing has grown considerably over the years. According to Anti-Phishing Working Group (APWG), the total number of phishing attacks in 2018. The total number of phish detected in 1Q 2018 was up 46 percent from the phish observed in 4Q 2017. It was also significantly more than what has been seen in 3Q 2017 (APWG report 2018). Phishing is one of the most predominant threats to organizations, and can cause important loss and instability. Phishers usually use human factors other than technological factors to hack people. To do so, they attempt to establish trust, or appeal to the recipient's emotions and values. During the past years, cryptography became more and more complicated and it becomes harder for hackers to use algorithmic hacking. Therefore, they rely more on social engineering and human factors. For example, today it is easier to obtain a password from a human by pretexting than breaking a security algorithm. Moreover, people usually overestimate their capacity to detect manipulation and deception (Wang et al. 2016, Sagarin et al. 2002). For example, Hong and al. (2013) found that out of 89% of recipients who thought were able to recognize phishing, only 7,5 % could really detect it. Janet and al. (2008) also showed that college students who were supposed to have a minimum education on cybersecurity cannot avoid to be trapped by phishing.

To develop effective programs to fight phishing, researchers have adopted behavioral approaches to understand recipients' motivations, and beliefs in phishing detection (Cialdini et al 2006; Hong 2012). In this research, we argue that individuals' initial emotions of a phishing email influences their behavioral reaction to the email's requests. The objective of the present study is to identify factors which can influence employees' phishing susceptibility to phishing emails. More specifically we investigate this phenomenon from recipients' emotions perspective.

2 Theoretical background

2.1 Why people might get deceived

Extant research mostly adopted psychological principles to explain why people might get deceived. For example, past research shows personal factors, and individuals' personality traits (i.e. neuroticism, extraversion, openness to experience, agreeableness, and conscientiousness) can impact the way users react to a phishing message (Parrish et al. 2009). Further, Vishwanath et al. (2016) showed that the capacity to detect a phishing message depends on the degree of cognitive effort someone takes to identify it. Their model accounted for cognitive processing, preconscious, and automatic behaviors that potentially lead to phishing based deception. They showed a higher level of heuristic processing would increase the likelihood to click a suspicious link. Moreover, automatism and habits increase the degree of individuals' suspicion about the veracity of a phishing email, whereas having a high cyber-risk belief decreases the risk to be deceived by phishing. Moreover, individuals' perception about the pertinence of an email to their needs and goals, and individuals' attention to phishing deception indicators (e.g. poor grammar and spelling mistakes) play important roles to detect a phishing email (Wang et al. 2012).

In an organizational context, past research emphasizes the roles of authority, commitment, trust, and reactance (i.e. scarcity and impulsivity) to explain the susceptibility to phishing (Workman 2008). According to the scarcity theory, opportunities seem more valuable when their availability are limited (Cialdini et al. 2006). Therefore, people might get deceived if they think by clicking on a malicious link they might achieve a "once-in-a-lifetime" opportunity.

2.2. Emotions and their influence on user behaviour

Emotions play an important role in people's decision and behaviour. Past studies argued that under some conditions emotions can have more power to explain behaviour than cognition (Zhang 2013). Emotions can be defined as "mental states of readiness that arise from the appraisal of events and one's own thoughts" (Bagozzi et al. 1999, p. 184). Moreover, cognitive appraisal theories argue that emotions reside between a person and a stimulus (Russel 2003). Stimulus is basically something or some event that a person reacts or responds to" (Zhang 2013, p. 250). For example, a subject line of an email can be a stimulus for the user and the emotion that is first triggered by reading the subject line can greatly impact whether the individual will open the email or delete it. In sum, emotions can be defined as affective states induced by or attributed to a specific stimulus. Emotions typically arise as reactions to situational events and objects in one's environment that are relevant to the needs, goals, or concerns of an individual" (Zhang 2013, p. 251). That is, people evaluate the stimulus and respond to it which can provoke certain emotions in them. Extant research showed that IT as a stimulus can trigger emotions and affect. Some studies relied on affective characteristics of stimulus (e.g. design characteristics) to explain emotional responses of users. For example, Ethier et al. (2006) showed website quality impacts customers' cognitive processes which evoke emotions like joy, liking, pride, dislike, and frustration.

In this research we argue that emotions play an important role in shaping employees' decision in responding to a phishing email. Basically, we argue that an IT stimulus which is related to employees' beliefs about their organizations can trigger emotions which eventually can influence their phishing susceptibility. Past research showed that in an organizational context, commitment to the organization, employees' obedience to authority, and resource scarcity can play important roles in increasing the risk of deception (Workman 2008). Following this line of thinking we argue that employees' emotional attachment to their organization (i.e. affective commitments), normative commitments, and sense of urgency (i.e. employees' perception of the need to respond quickly), can evoke emotional reactions in employees while they receive a phishing message, and in turn, those emotions can influence employees' phishing susceptibility.

3 Conceptual Framework

Our framework (see Figure 1) proposes that in an organizational context when employees receive a phishing email which pretends to be from their organization, their emotional attachment to their organization, their normative commitment, and their perception of the urgency of the email can evoke contentment and anxiety, which in turn can influence the probability of getting deceived by the email. The constructs and their definitions are explained in Table 1.

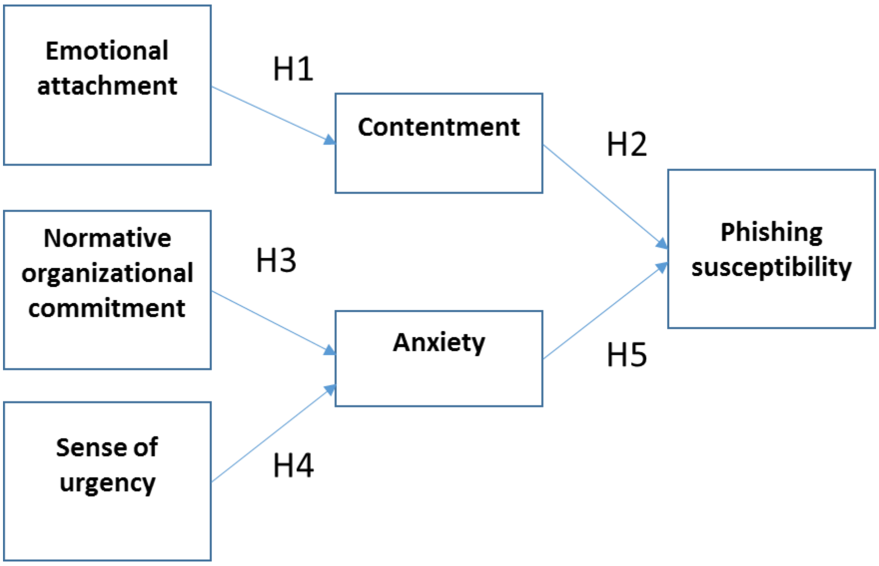

Figure 1. Conceptual model

Construct	Definition	Reference
Normative organizational commitment	Employees' perceptions of their obligation to their organization.	(Allen and Meyer 1990)
Emotional attachment to the organization	An employee who is emotionally attached to the organization strongly identifies with the goals of the organization and desires to remain a part of the organization. This employee commits to the organization because he/she wants to.	(Allen and Meyer 1990)
Sense of urgency	A felt need to initiate and complete an act in an immediate or near future	(Swain et al. 2006)
Susceptibility to phishing emails	The probability that an employee be deceived by a targeted phishing email.	(Workman 2008)

Table 1. Constructs and their definitions

3.1. Emotional attachment to organizations

The concept of organizational emotional attachment underlies the fact that an employee develops an affectional attachment to his or her organization. Thus, employees who have a strong level of affective commitment identify organizations missions and values as their own. Such employees are implicated in the organization, are happy to be members of the organization for which they work, and they do everything they can to produce the most valuable work for their organization (Meyer and Allen 1997). That is, employees with such characteristics identify themselves with their organization. Past research on organizational identification suggests that such a belief has an implication for emotion experienced in the interaction with the organization (Anderson and Chen 2002, Chen et al. 2006). Moreover, past research suggests that those with higher identification tend to experience more intense emotions (Smith et al. 2007). Drawing from this research, we hypothesize that employees’ attachment to theor organization is associated with emotions generated while receiving an email from their organization. More specifically, we argue that emotional attachment and the feeling of belonging can increase employees’ contentment and happiness. This is also inline with past research that shows affective organizational commitment is correlated with experiencing positive emotions (Herrbach 2006). Hence, H1: Employees who have higher emotional attachment to their organization will feel more contentment as they perceive the phishing email to be from their organization.

Research in psychology found that emotional states exert significant effects on memory, judgment, and decision making (Martin and Clore, 2001). Some studies suggest that certain positive emotions lead people to rely more on highly accessible cognitions, such as beliefs and expectations (Forgas and Fiedler 1996). Also past research showed that people who experienced positive moods might produce less persuasive arguments which may be, in part, because positive emotions arise in a safe environment. Therefore, under some conditions, happiness can increase the likelihood of making fundamental attribution errors (Forgas, 1998). Such heuristic information processing tendencies, therefore, may not be beneficial when there is a need for analytic processing (e.g. detecting a phishing email). Drawing from this research, we hypothesize that employees' contentment when they receive a phishing email can increase the probability of their deception since they feel safe. Hence,

H2: The feeling of contentment triggered by a phishing email will increase employees' phishing susceptibility.

3.2. Normative organizational commitment

Normative organizational commitment is a concept that was introduced by Allen and Meyer (1990). It refers to the idea that employees feel obliged to develop loyal behaviour to their organization, in particular by adhering to its standards and values. Meyer and Allen (1991) argue that this concept emerges due to the process of socialization and internalization of normative pressures exerted on the individual. People with higher normative commitment are usually more obedient to authority and they would feel anxious if they do not follow the rules and requests. We argue that an employees' degree of normative commitment to an organization can increase their anxiety as they notice that the email is sent by their organization, since they see themselves obliged to answer organization's requests. Hence,

H3: Employees who have higher normative organizational commitment will feel more anxiety as they perceive the phishing email is from their organization.

3.3. Sense of urgency

Sense of urgency has been defined as a felt need to initiate and complete an act in an immediate or near future (Swain et al. 2006). Hence, an individual exhibiting an urge is not likely to postpone the action to gather more information, indulge in comparison, and seek advice. The sense of urgency basically is individual' psychological responses to the scarcity environments (Brehm 1966). Scarcity that is communicated by the phisher threatens users' freedom, thus triggering psychological reactance and encouraging them to take immediate actions. The scarcity is usually communicated to the user by convincing the user that he/she has a limited time to reply, if not he/she might lose an opportunity or experience adverse effects (e.g. penalized). Therefore, people may react quickly and at time illogically to perceived shortage in order to restore the lost freedom (Brehm 1966). Extant research in marketing shows that scarcity messages (for example, time restricted promotional messages) affect consumers' purchase intentions by affecting not only the outcomes, but also consumers' emotions (Swain, et al. 2006). Drawing from this research we hypothesize that if employees perceive a message to be urgent and from their organization, they become anxious. In turn, the anxiety can increase the probability of their deception which might lead to answering the phishing email. Hence,

H4: Employees who perceive a phishing message to be more urgent, will feel more anxiety.

H5: The feeling of anxiety triggered by a phishing email will increase employees' phishing susceptibility.

4 Proposed Methodology

In this research, we aim to measure the susceptibility of employees to phishing when they receive a fake e-mail from their organization. To do so, we will use a survey methodology and we aim to collect data from members of a multi-university association. To measure the phishing susceptibility of the members, we will create a phishing email that asks respondents (i.e. members of the association) to click on a link in the body of the email. The email seems to be from the previous president of the organization and asks respondents to click on a link which invites them to register for an urgent and important meeting. The email has five stimuli, which tries to convince the respondent about the originality of it. As shown in Table 2, each stimulus can be associated with one or more constructs. The email will appear as the first question of the survey and then the respondents will be asked about the likelihood of clicking on the link in the body of the email is they happen to receive such an email. Following this question, the three main constructs of the research (i.e. emotional attachment to the organization, normative commitment, and sense of urgency) will be measured. We aim to analyse data using structural equation modelling techniques.

Stimulus	**Related constructs**
Stimulus 1: To convince the participants that the email is from the "Association", we put "Association" in the email address to reinforce the deception. Having access to an organizational address increases the success of a phishing attack.	Emotional attachment
Stimulus 2: We pretend that the sender of the email is someone who is the past-president of the organization.	Emotional attachment
Stimulus 3: The subject of the email is "an urgent meeting".	Normative commitment, sense of urgency
Stimulus 4: The e-mail has a deadline which implies the urgency of the answer.	Sense of urgency
Stimulus 5: The phrases and tone used were normative which oblige members to participate in the meeting.	Normative commitment.

Table 2. Email stimuli and their related constructs

5 CONCLUSION

Employees' deception by phishing emails is a threat to organizations. Past research showed the role of organizational commitment, authority, and perceived resource scarcity in employees' decision to respond to such emails. Drawing from past research, we argue that employees' emotions play a mediating role and "organizational emotional attachment", "normative commitment", and "sense of urgency" can lead to emotions of contentment and anxiety which in turn will influence employees' phishing susceptibility. In future steps, we plan to test our model by using a survey methodology.

References

Allen, N.J., and Meyer, J.P. 1990. "The Measurement and Antecedents of Affective, Continuance and Normative Commitment to the Organization," *Journal of occupational and organizational psychology* (63:1), pp. 1-18.

Anti-Phishing Working Group. Phishing activity trends report. In APWG (ed.), Anti-Phishing Working Group, 2018. Available at: http://docs.apwg.org/reports/apwg_trends_report_q1_2018.pdf (accessed on May 15, 2019)

Bagozzi, R.P., Gopinath, M., and Nyer, P.U. 1999. "The Role of Emotions in Marketing," *Journal of the academy of marketing science* (27:2), pp. 184-206.

Cialdini, R.B., Demaine, L.J., Sagarin, B.J., Barrett, D.W., Rhoads, K., and Winter, P.L. 2006. "Managing Social Norms for Persuasive Impact," *Social influence* (1:1), pp. 3-15.

Éthier, J., Hadaya, P., Talbot, J., and Cadieux, J. 2006. "B2c Web Site Quality and Emotions During Online Shopping Episodes: An Empirical Study," *Information & Management* (43:5), pp. 627-639.

Forgas, J.P. 1998. "On Being Happy and Mistaken: Mood Effects on the Fundamental Attribution Error," *Journal of personality and social psychology* (75:2), p. 318.

Forgas, J.P., and Fiedler, K. 1996. "Us and Them: Mood Effects on Intergroup Discrimination," *Journal of Personality and Social Psychology* (70:1), p. 28.

Herrbach, O. 2006. "A Matter of Feeling? The Affective Tone of Organizational Commitment and Identification," *Journal of Organizational Behavior* (27:5), pp. 629-643.

Hong, K.W., Kelley, C.M., Tembe, R., Murphy-Hill, E., and Mayhorn, C.B. 2013. "Keeping up with the Joneses: Assessing Phishing Susceptibility in an Email Task," *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*: SAGE Publications Sage CA: Los Angeles, CA, pp. 1012-1016.

Janet, L., Mitchell, D., Robert, B., and Bradley, K. 2008. "Analysis of Student Vulnerabilities to Phishing," *AMCIS 2008 Proceedings*), p. 271.

Jensen, M., Durcikova, A., and Wright, R. 2017. "Combating Phishing Attacks: A Knowledge Management Approach," *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Martin, L.L., and Clore, G.L. 2013. *Theories of Mood and Cognition: A User's Guidebook*. Psychology Press.

Meyer, J.P., and Allen, N.J. 1991. "A Three-Component Conceptualization of Organizational Commitment," *Human resource management review* (1:1), pp. 61-89.

Meyer, J.P., Allen, N.J., and Allen, N.J. 1997. *Commitment in the Workplace*. Sage Publications.

Parrish Jr, J.L., Bailey, J.L., and Courtney, J.F. 2009. "A Personality Based Model for Determining Susceptibility to Phishing Attacks," *Little Rock: University of Arkansas*).

Russell, J.A. 2003. "Core Affect and the Psychological Construction of Emotion," *Psychological review* (110:1), p. 145.

Sagarin, B.J., Cialdini, R.B., Rice, W.E., and Serna, S.B. 2002. "Dispelling the Illusion of Invulnerability: The Motivations and Mechanisms of Resistance to Persuasion," *Journal of personality and social psychology* (83:3), p. 526.

Swain, S.D., Hanna, R., and Abendroth, L.J. 2006. "How Time Restrictions Work: The Roles of Urgency, Anticipated Regret, and Deal Evaluations," *ACR North American Advances*).

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.

Wang, J., Chen, R., Herath, T., and Rao, H.R. 2009. "An Exploration of the Design Features of Phishing Attacks," *Information Assurance, Security and Privacy Services* (4), p. 29.

Wang, J., Herath, T., Chen, R., Vishwanath, A., and Rao, H.R. 2012. "Research Article Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email," *IEEE transactions on professional communication* (55:4), pp. 345-362.

Workman, M. 2008. "Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security," *Journal of the Association for Information Science and Technology* (59:4), pp. 662-674.

Zhang, P. 2013. "The Affective Response Model: A Theoretical Framework of Affective Concepts and Their Relationships in the Ict Context," *MIS Quarterly* (37:1), pp. 247-274.