Research Report

Phish Me If You Can: Insights from an Eye-Tracking Experiment

PHISHING E-MAILS CONTINUE TO POSE A TOP THREAT TO AN ORGANIZATION'S INFORMATION SECURITY. DESPITE TECHNICAL ADVANCES, THE BURDEN OF DETECTING AND DEALING WITH THEM ULTIMATELY REMAINS ON THE SHOULDERS OF THE INDIVIDUAL EMPLOYEE. THIS ARTICLE PRESENTS RESULTS OF A MULTI-METHOD PHISHING EXPERIMENT INCLUDING THE USE OF AN EYE-TRACKING DEVICE TO ASSESS EMPLOYEES' ACTUAL AWARENESS OF PHISHING AND INFLUENCING FACTORS. PRACTICAL IMPLICATIONS FOR SECURITY TRAININGS ARE ALSO DISCUSSED.

Lennart Jaeger

Andreas Eckhardt

Introduction

Information is central to the functioning of modern organizations and the most important factor holding organizations together. This centrality ultimately gives information critical value, and safeguarding information has become a top management priority in many organizations. Yet, as a consequence of an increasingly connected world and the strong dependence on information systems, organizations are continually finding it difficult to keep their information assets secure. Many notorious security incidents in the recent past show that security attacks from outside the organization as well as employees' misbehavior inside the organization can have grave consequences, including corporate liability, loss of reputation, and financial damage. To ensure information security, organizations have often relied only on technology-based solutions in the past, such as antivirus software, firewall management systems, or intrusion detection systems. But the sole reliance on these types of solutions is not sufficient because it is estimated that 47-60% of all security incidents are either directly or indirectly due to employee misconduct (Verizon, 2020).

As the focus of information security continues to shift towards individual and organizational perspectives, organizations realize that employees, often considered as the 'weakest link' in the information security chain, can also be vital assets to reduce security risks. Because individuals who are aware of their organization's security mission and ideally committed to it are the key to strengthening information security, understanding *information security awareness* (hereinafter: ISA) is vital for organizations that want to leverage their human capital (Bulgurcu et al., 2010). Accordingly, in realizing the dual role of their employees, as both allies and sources of security threats, organizations have started to invest in security education, training, and awareness programs to ensure that their employees have an appropriate level of knowledge about information security along with an appropriate sense of responsibility. However, the unabated prevalence of information security incidents due to employees' intentional or unintentional actions shows that reality still falls short of this ideal.

In phishing, for example, the burden of detecting and coping with phishing mails ultimately remains on the shoulders of the individual employee. Questions about why phishing works are fundamentally questions about awareness: When individuals fall for a phishing mail, did they deliberately assess the situation (e.g., check sender address) or did they click on it without much deliberate thought (Dennis and Minas, 2018)? To answer this question, studies have mainly investigated the impact of E-mail recipients' characteristics, and the characteristics of the E-mail itself. However, research has largely overlooked interactions between the recipient of a phishing mail and the situation the recipient is in, i.e., the moment when an individual processes an E-mail.

Thus, since the full extent of individuals' actual awareness in a security-related situation remains to be clarified, we introduce the concept of *situational* ISA as individuals' knowledge of particular security threats transported by security-related information cues captured in a situational process in the immediate system environment. Our research aims to empirically examine determinants and consequences of individuals' situational ISA.

Phishing Eye-Tracking Experiment

We conducted an experimental study in the context of E-mail communication, in which participants received a mailbox exercise. Participants took the role of an employee in a fictitious organization and read and processed 20 E-mails, including six phishing mails, stored in a webmail inbox. The phishing mails varied in contextual relevance (i.e., the alignment with recipients' work responsibilities) and misplaced salience (i.e., salient design features including colored text, logos, buttons, and pictures). The experiment was conducted with 107 employees from various organizations. 55% of them were men and the average participant was 40 years in age, used a computer at work for 6.6 hours per day, and had 3.4 E-mail accounts.

An eye-tracking device was used to record participants' eye movements to security cues (e.g., sender address, real URL link, file info of attachment, etc.). Situational ISA was measured by the number of security cues that

individuals paid attention to compared to all available security cues. In other words, the more they looked at, the better. As visualization, Figure 1 provides an example of someone with a high degree (left) and of someone with a low degree of situational ISA (right). Blue dots and lines are the areas participants looked at. Differently colored squares represent the security cues. Security-related behavior was measured by coding protective actions taken during the experiment including whether participants deleted/archived the phishing mail or notified the helpdesk, whereas clicking on a phishing link or downloading an attachment was considered as unsafe behavior. After participants processed the 20 E-mails, they filled out a questionnaire to capture other variables of interest for the study.

Empirical Findings

We found that, in 26% of all cases, participants clicked on the enclosed links or downloaded the attachment in the phishing mails. This result is in line with industry experiences and phishing benchmarking studies (KnowBe4, 2018). Furthermore, in a quarter of those cases, login data was submitted or the attachment opened. On the other hand, in 38% of all cases, participants deleted the phishing mail or archived it in the spam folder, while in only 8% of all cases participants reported the phishing mail to the IT helpdesk. To explain such security-related behaviors, we developed and empirically tested a model of situational ISA (see Figure 2) by drawing on prior research of situation awareness, phishing literature, and protection motivation theory as applied in information security (Boss et al., 2015). We integrate key factors which draw on the interaction between the individual employees and their system environment in achieving situational ISA.

At the individual level, prior experience with phishing positively influences situational ISA (*H1*). Experienced individuals demonstrate their awareness by attending to more security cues. This suggests that experience enables the development of schemata and recognizing the critical cues that activate pattern matching of the phishing mail with schemata in the process of forming awareness.

Contrary to what we expected, the personality trait of agreeableness did not significantly impact situational ISA (*H2*). Although agreeable individuals tend to be more trustworthy and susceptible to phishing, in our case, it did not lead to paying less attention to security cues. However, agreeable individuals could still fall for a phishing mail by being influenced by compelling parts of the E-mail text rather than security cues.

At the system level, situational ISA is negatively influenced by contextual relevance (*H3*) and misplaced salience (*H4*). When the premise of a phishing mail is aligned to their work context, individuals pay attention to fewer information security-related cues in phishing messages. Moreover, when phishing mails have salient design elements, such as logos, images, or buttons, they direct attention more

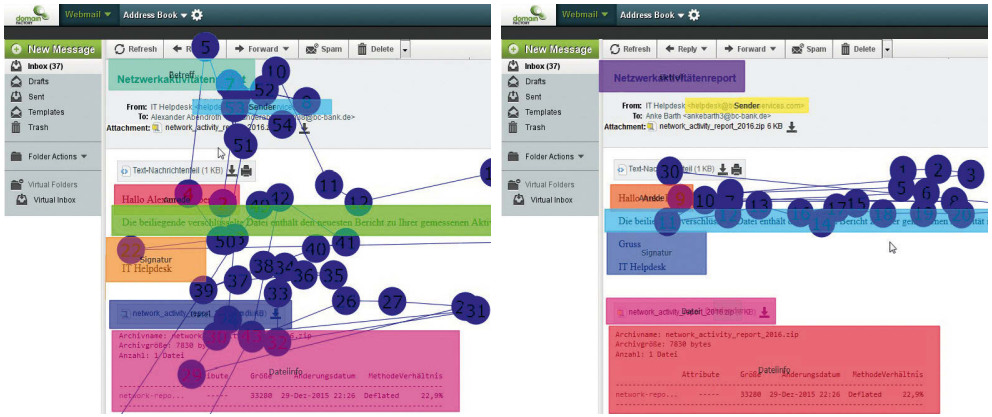

Figure 1: Gaze Plot Comparison (adapted from Jaeger and Eckhardt, 2020)

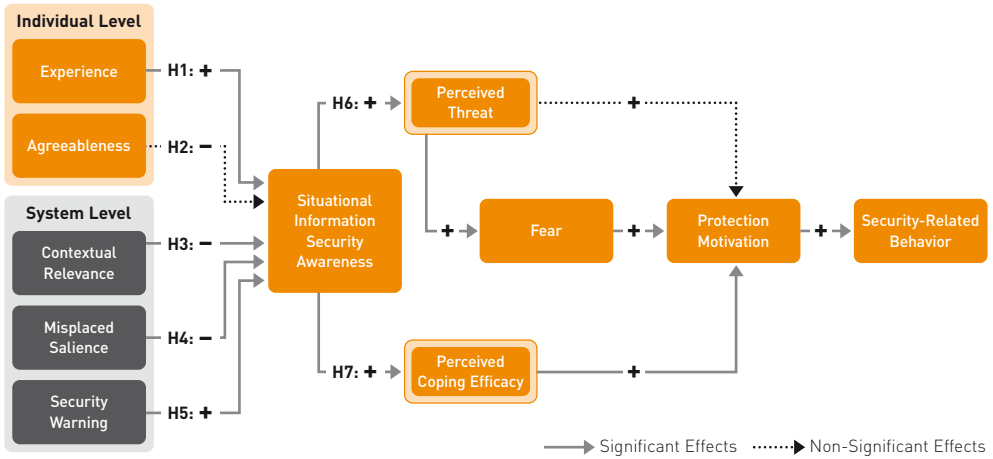

Figure 2: Research Model of Situational Information Security Awareness

away from security cues than E-mails with just plain text.

Moreover, a security warning raises individual's situational ISA (*H5*). Participants who received a security warning during the experiment attended to more security cues. This indicates that warnings can serve as a critical cue to activate the mechanisms of matching the pattern of a phishing mail with existing schemata.

Regarding the consequences of situational ISA, we find that it influences both the development of threat and coping appraisals. Situational ISA is a significant determinant for perceived threat (*H6*). Since security cues, like the file extension of an attachment (e.g., .exe), may indicate whether opening such attachments may lead to the corruption of data, examining such cues provides an informational basis to evaluate how threatening an E-Mail is.

Additionally, while there was no direct influence of perceived threat on protection motivation, we find an indirect influence through individual's fear of phishing. In other words, when individuals see phishing as threatening, the fear of phishing is generated as an outcome, which also raises their motivation to take protective actions against phishing, termed protection motivation.

Regarding coping appraisal, we find that individuals who paid attention to more security cues, also feel more confident to take relevant actions and perceive that these actions are effective, taken together termed perceived coping efficacy (*H7*). This also raises their protection motivation. Protection motivation ultimately increases security-related behaviors, such as deleting the phishing mail or notifying the helpdesk.

Implications for Practitioners

Our findings have important practical implications for information security management. Individuals with phishing experience pay attention to more security cues, such as sender address or real URL links. This indicates that their mental models of phishing are more complex and contain more links between concepts related to the characteristics of phishing attacks than those with less phishing experience. Accordingly, training programs should be designed to provide information about the interconnectedness of security cues; for example, how an unknown sender may be connected with an impersonal greeting, which could be related to a malicious attachment or fake link.

The negative impact of a phishing mail's contextual relevance on situational ISA emphasizes the importance of varying phishing exercises suitably and challenge employees with contextually relevant E-mails to provide training on new scams. Training implementers must understand the relevancy of a phishing mail for their trainees. For example, certain work groups may have to regularly interact with external third parties and may be more exposed, which could make them more susceptible to phishing. On the other hand, they could actually be the ones that acquire situational ISA more easily. This is due to the fact that they have to regularly match patterns of E-mails with their mental library of what an E-mail should look like to determine whether it is a legitimate or phish.

To manage different abilities, the used training set of phishing mails should differ in their detection difficulty by varying the number of security cues that are manipulated (e.g., is only the sender address and link fake, or also other parts in the message). More experienced or frequently exposed work groups may benefit from a variation of more difficult phishing mails that update and enhance their mental models of phishing and counter possible stereotypes that may develop by being repeatedly exposed to similar phishing mails. Conversely, less experienced or exposed work groups may respond more favorably to more simple phishing mails with fewer cues being manipulated to initially help them develop a mental library of prototypical phishing mails.

References

Boss, S. R.; Galletta, D. F.; Lowry, P. B.; Moody, G. D.; Polak, P.:
What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear That Motivate Protective Security Behaviors.
In: MIS Quarterly, 39 (2015) 4, pp. 837–864.

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

Dennis, A. R.; Minas, R. K.:
Security on Autopilot: Why Current Security Theories Hijack our Thinking and Lead Us Astray.
In: ACM SIGMIS Database, 49 (2018) 1, pp. 15–38.

Jaeger, L.; Eckhardt, A.:
Eyes Wide Open: The Role of Situational Information Security Awareness for Security-Related Behaviour.
In: Information Systems Journal, 31 (2021) 3, pp. 429-472.

KnowBe4:
Report 2018: Phishing by Industry Benchmarking, https://info.knowbe4.com/2018-phishing-by-industry-benchmarking-report, 2018.

Verizon:
2020 Data Breach Investigations Report, https://enterprise.verizon.com/resources/reports/dbir, 2020.