Contextual Influences on Phishing Susceptibility: A Qualitative Comparative Analysis

Fabian Hable
KIN Center for Digital Innovation
Vrije Universiteit Amsterdam, Netherlands

Nina-Birte Schirrmacher
KIN Center for Digital Innovation
Vrije Universiteit Amsterdam, Netherlands

Bart van den Hooff
KIN Center for Digital Innovation
Vrije Universiteit Amsterdam, Netherlands

ABSTRACT

Phishing represents a pervasive form of social engineering, whereby the objective is to gain access to sensitive personal information through the use of deceptive emails. Despite extensive research on the internal factors – those inherent to the prospective target and beyond the control of organizational interventions – influencing phishing susceptibility, there has been comparatively little investigation of the external factors in a corporate setting. This study examined the influence of external factors, such as organizational context, environmental conditions, and the phishing attack itself, on phishing susceptibility within a corporate context. Towards this, a phishing campaign was conducted in a European-based manufacturing company. To identify all relevant external factors, we conducted interviews with employees targeted by the campaign and used a grounded theory approach. Next, we will investigate how configurations of external factors influence employee phishing susceptibility using a fuzzy-set qualitative comparative analysis (fsQCA). Thereby, this study seeks to contribute to the literature on phishing susceptibility.

Keywords: Phishing susceptibility, phishing attack context, organizational context, situational context, qualitative comparative analysis

INTRODUCTION

Phishing is a form of social engineering, in which attackers primarily seek to commit identity theft by acquiring sensitive personal information, such as login credentials, for financial gain or reputational damage to their targets (Greene et al. 2018; Mitnick and Simon 2003; Wang et al. 2021). Email phishing is the practice of sending deceptive emails that contain links to fake

websites that look like legitimate ones. The growth in phishing attacks is alarming, with 2022 marking a record year with over 4.7 million attacks and an annual increase of more than 150% since 2019 (APWG 2022). 95% of successful cyberattacks are due to human error (IBM 2019), underscoring the critical importance of understanding what shapes phishing susceptibility.

The majority of extant research on phishing susceptibility has concentrated on either the phishing email attack itself or on the targets' inherent factors such as personality traits, cognitive biases or cognitive processing (Frauenstein et al. 2023; Rahman et al. 2022; Wright et al. 2010). For example, individuals who engage in heuristic processing (rapid, automatic decision-making) are more prone to fall prey to phishing emails due to a reduction in critical analysis (Ayaburi and Andoh-Baidoo 2019; Frauenstein et al. 2023).

While internal factors have been extensively studied, external factors, or contextual aspects that vary depending on the situation in which a phishing attack occurs, remain relatively understudied. External factors, such as organizational context, environmental conditions, and the phishing attack context itself, are beyond the individual's control. Only a limited number of studies have examined the influence of external factors, including corporate training, workload or organizational environment, on phishing susceptibility (Caputo et al. 2014; Jaeger and Eckhardt 2021; Wright et al. 2023).

The majority of studies on external factors influencing phishing susceptibility have employed a quantitative methodology and were conducted in a university setting or with Amazon Mechanical Turk (Butavicius et al. 2022; Vishwanath et al. 2011; Williams et al. 2017). These studies concentrate on individuals outside the work environment rather than on employees in organizations, which may limit the insights that their findings provide into the role of the situational work context. Understanding external factors in the workplace is crucial, as

employees are confronted with more significant challenges, a variety of pressures, and a greater degree of responsibility compared to the relatively homogeneous environment of a university setting.

To better understand external factors influencing phishing susceptibility, more studies in corporate settings with real phishing campaigns are needed. We conducted a qualitative study in an organizational setting using grounded theory and comparative qualitative analysis (QCA) to explore the possibility of additional external factors to literature. Furthermore, we aim to investigate how these factors interact and influence behavior during a phishing attack, thereby providing a more comprehensive understanding of the external dynamics at play. Therefore, this study aims to address the following two research questions:

- Which external factors influence an individual's response to a phishing email in an organizational setting?
- How does the interplay between external factors influence an individual's response to a phishing email in an organizational setting?

Thereby, this study makes two contributions to the existing literature on phishing susceptibility. First, this study will offer a more profound comprehension of the impact of external factors in an organizational setting on an employee's phishing susceptibility. Secondly, by employing a QCA in a corporate context, this research will illustrate combinations of external factors which lead to phishing susceptibility. In essence, this approach strives to offer a comprehensive understanding of the intricate relationship between external factors and phishing susceptibility, thereby providing novel theoretical and practical insights.

THEORETICAL BACKGROUND

Phishing research defines "susceptibility" through actions like clicking on a phishing link or providing personal credentials (Abbasi et al. 2021; Butavicius et al. 2022; Jaeger and Eckhardt 2021). Some studies equate susceptibility with clicking (Moody et al. 2017), while others include disclosing credentials on fraudulent sites (Jensen et al. 2017; Wright et al. 2014, 2023). Clicking shows initial engagement, while providing credentials represents a deeper level of deception.

Phishing susceptibility is influenced by a number of factors, both internal and external. Internal factors include cognitive biases and personality traits, while external factors encompass the organizational environment, workload, and characteristics of phishing emails. This research focuses on the external factors, which are beyond the control of the individual, and their relationship to both the attack and the organization. The following sections examine the impact of these external factors on phishing susceptibility.

Attack-Related Factors

Phishing attacks typically commence with the dissemination of deceptive emails, which are crafted with the intention of persuading targets that the message is authentic. In a manner similar to marketing, phishing emails employ persuasive tactics with the objective of prompting actions such as clicking on malicious links or providing sensitive information (Cialdini 2001). These tactics often rely on Cialdini's principles of persuasion: reciprocity, commitment/consistency, social proof, authority, liking or scarcity (Cialdini 2001). For example, the presence of authority figures can enhance the perceived credibility of a message, thereby reducing skepticism or the liking principle in phishing messages exploits the tendency of targets to comply with requests from those they perceive as familiar or likable (Garcia and Parra 2021; Lin et al. 2019; Qahri-Saremi and Turel 2023; Workman 2008; Wright et al. 2014).

External Factors at the Organizational Level

In organizational settings, external factors such as reliance on IT support, time pressure, and learning experiences play a significant role in shaping susceptibility to phishing, rendering these environments more complex than university studies (Frank et al. 2022; Wright et al. 2023). For instance, those who rely heavily on IT support, and those who are less central to work-task networks are more susceptible to phishing attacks. Conversely, trust in formal platforms like help desks has been shown to reduce the risks associated with phishing (Frank et al. 2022; Wright et al. 2023). Furthermore, high time pressure and low resilience have been identified as factors that contribute to increased susceptibility (Wright et al. 2023). Prior phishing experience has been shown to reduce susceptibility (Jaeger and Eckhardt 2021). The effectiveness of training varies, with some employees demonstrating a tendency to disregard the content of the training (Caputo et al. 2014).

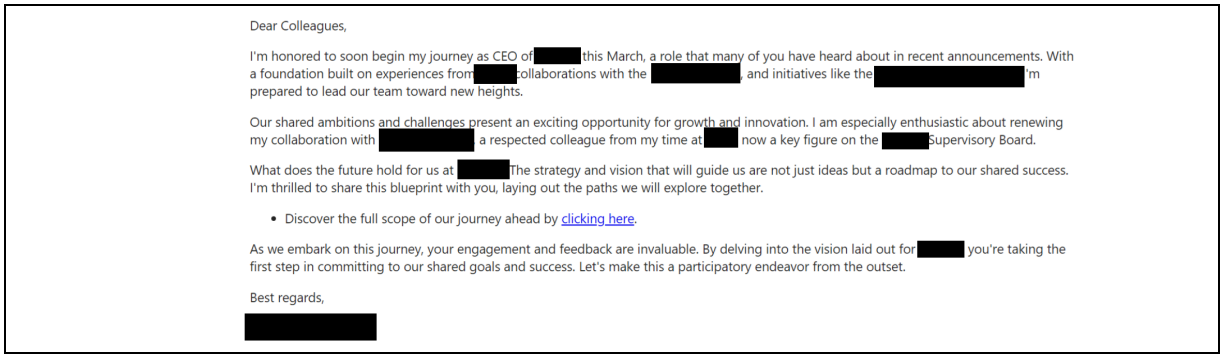
All in all, the literature provides some first insight into which external factors may influence phishing susceptibility, but does not yet provide an in-depth understanding of how these factors interact in shaping susceptibility.

METHOD

Study Design

The phishing campaign was a field experiment whereby phishing emails, appearing to be from the company's recently appointed CEO, were sent to employees (see Figure 1). This allowed for the study of employee behavior in a controlled setting. The email was constructed using artificial intelligence, publicly accessible data, and persuasion principles such as authority and urgency (Cialdini 2001). The employees were invited to review the CEO's vision via a link, which led to a Microsoft login page that imitated the company's standard practice. The phishing

page proceeded to tunnel requests to the legitimate Microsoft site, thereby enabling us to see which employee provided credentials. Of the 399 employees, 370 received the email, with 77 clicking the link and 37 providing their credentials. This approach yielded valuable insights into phishing susceptibility while reinforcing cybersecurity awareness without causing actual harm.



Dear Colleagues,

I'm honored to soon begin my journey as CEO of [redacted] this March, a role that many of you have heard about in recent announcements. With a foundation built on experiences from [redacted] collaborations with the [redacted], and initiatives like the [redacted] I'm prepared to lead our team toward new heights.

Our shared ambitions and challenges present an exciting opportunity for growth and innovation. I am especially enthusiastic about renewing my collaboration with [redacted] a respected colleague from my time at [redacted] now a key figure on the [redacted] Supervisory Board.

What does the future hold for us at [redacted] The strategy and vision that will guide us are not just ideas but a roadmap to our shared success. I'm thrilled to share this blueprint with you, laying out the paths we will explore together.

- Discover the full scope of our journey ahead by clicking here.

As we embark on this journey, your engagement and feedback are invaluable. By delving into the vision laid out for [redacted] you're taking the first step in committing to our shared goals and success. Let's make this a participatory endeavor from the outset.

Best regards,

[redacted]

Figure 1. Phishing E-Mail of the Phishing Campaign

Data Collection

In this study, phishing susceptibility was defined as instances where targets clicked on a phishing link and provided their login credentials, thereby allowing unauthorized access to their account. 31 employees were interviewed, 19 of whom had been successfully deceived by the phishing email, while 12 remained uncompromised and have not clicked on the link. The interviews investigated the targets' memory of the attack, including the impact of email characteristics, work environment during the attack, emotional states, distractions, prior phishing experiences, and the efficacy of cybersecurity training. Conducted primarily in German, all interviews were transcribed and translated into English for analysis.

Data Analysis

We used ATLAS.ti for inductive data analysis to examine why successfully phished targets responded to our phishing email, focusing on the external causes which led to provided credentials. Subsequently, an analysis was conducted on the identified factors from the group of targets that had been trapped, in addition to a comparison group of targets that had not been

trapped. In a next step, the Gioia approach was subsequently employed to identify patterns and group similar first-order concepts into second-order themes, and finally categorizing these themes into three dimensions: attack context, situational context, and organizational context (Gioia et al. 2013) (see Figure 2).

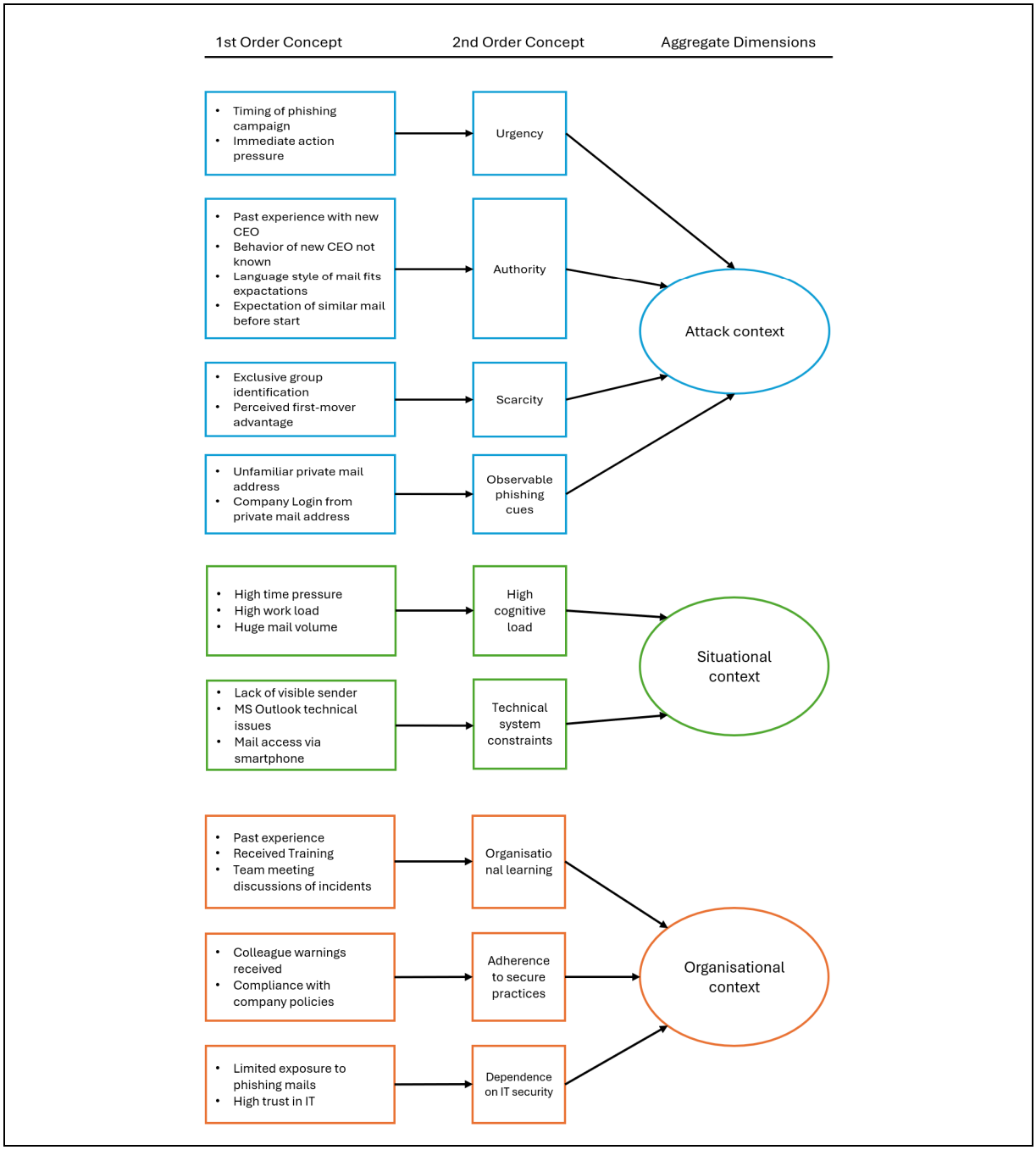


Figure 2. Data structure

Qualitative Comparative Analysis

QCA is a method used to identify patterns across cases by examining combinations of factors that lead to specific outcomes (Mattke et al. 2022). In the present study, we will employ QCA in order to ascertain how the various external factors, identified via our Gioia approach, interact in order to influence phishing susceptibility. Unlike traditional variable-centered methods, QCA allows for the identification of combinations of factors that lead to a successful phishing attempt (provision of credentials) or resistance (no click).

Each interview will be assessed individually, indicating the presence or absence of the second-order concepts identified in the Gioia analysis (see Figure 2). This approach allows us to evaluate not only the individual impact of external factors (independent variables), but also how different combinations of these factors relate to phishing susceptibility. For instance, factors identified from the Gioia method include high cognitive load, or dependence on IT security.

Each factor will be calibrated to a fuzzy set format, whereby a value of 1 will be assigned if the factor was present and 0 if it was absent. The calibration process will entail a review of the interview data and an assessment of the presence of each factor based on the context described by the interviewee. The calibration data will then be summarized in a truth table, which is a fundamental component of QCA methodology (Mattke et al. 2022). This table encompasses all potential configurations of the factors and outcomes across all cases.

We will then reduce the truth table to the most relevant configurations that explain phishing susceptibility. This process will facilitate the isolation of the primary combinations of factors that result in provision of credentials or no click. Finally, the minimal solutions will be evaluated to determine their theoretical validity and practical significance.

REFERENCES

Abbasi, A., Dobolyi, D., Vance, A., and Zahedi, F. M. 2021. "The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites," *Information Systems Research* (32:2), pp. 410–436.

APWG. 2022. "Phishing Activity Trends Report," (https://apwg.org/trendsreports)

Ayaburi, E., and Andoh-Baidoo, F. K. 2019. "Understanding Phishing Susceptibility: An Integrated Model of Cue-Utilization and Habits," *Proceedings of the International Conference on Information Systems* (43).

Butavicius, M., Taib, R., and Han, S. J. 2022. "Why People Keep Falling for Phishing Scams: The Effects of Time Pressure and Deception Cues on the Detection of Phishing Emails," *Computers & Security* (123), p. 102937.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., and Johnson, M. E. 2014. "Going Spear Phishing: Exploring Embedded Training and Awareness," *IEEE Security & Privacy* (12:1), pp. 28–38.

Cialdini, R. B. 2001. "The Science of Persuasion," *Scientific American* (284:2), pp. 76–81.

Frank, M., Jaeger, L., and Ranft, L. M. 2022. "Contextual Drivers of Employees' Phishing Susceptibility: Insights from a Field Study," *Decision Support Systems* (160), p. 113818.

Frauenstein, E. D., Flowerday, S., Mishi, S., and Warkentin, M. 2023. "Unraveling the Behavioral Influence of Social Media on Phishing Susceptibility: A Personality-Habit-Information Processing Model," *Information & Management*, p. 103858.

Garcia, V.A. and Parra, R.D., 2021. "Phishing video game to validate the principles of persuasion in university students." In *AMCIS*.

Gioia, D. A., Corley, K. G., and Hamilton, A. L. 2013. "Seeking Qualitative Rigor in Inductive Research: Notes on the Gioia Methodology," *Organizational Research Methods* (16:1), pp. 15–31.

Greene, K., Steves, M., Theofanos, M., and Kostick, J. 2018. "User Context: An Explanatory Variable in Phishing Susceptibility," in *Proceedings 2018 Workshop on Usable Security*, San Diego, CA: Internet Society.

IBM. 2019. "Cost of a data breach report," (https://www.ibm.com/security/data-breach)

Jaeger, L., and Eckhardt, A. 2021. "Eyes Wide Open: The Role of Situational Information Security Awareness for Security-related Behaviour," *Information Systems Journal* (31:3), pp. 429–472.

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.

Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., and Ebner, N. C. 2019. "Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content," *ACM Transactions on Computer-Human Interaction* (26:5), 32:1-32:28.

Mattke, J., Maier, C., Weitzel, T., Gerow, J. E., and Thatcher, J. B. 2022. "Qualitative Comparative Analysis (QCA) In Information Systems Research: Status Quo, Guidelines, and Future Directions," *Communications of the Association for Information Systems* (50), pp. 208–240.

Mitnick, K. D., and Simon, W. L. 2003. "The Art of Deception: Controlling the Human Element of Security," *John Wiley & Sons*.

Moody, G. D., Galletta, D. F., and Dunn, B. K. 2017. "Which Phish Get Caught? An Exploratory Study of Individuals′ Susceptibility to Phishing," *European Journal of Information Systems*.

Qahri-Saremi, H., and Turel, O. 2023. "Situational Contingencies in Susceptibility of Social Media to Phishing: A Temptation and Restraint Model," *Journal of Management Information Systems* (40:2), pp. 503–540.

Rahman, A. U., Al-Obeidat, F., Tubaishat, A., Shah, B., Anwar, S., and Halim, Z. 2022. "Discovering the Correlation Between Phishing Susceptibility Causing Data Biases and Big Five Personality Traits Using C-GAN," *IEEE Transactions on Computational Social Systems*, pp. 1–9.

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, Z., Zhu, H., and Sun, L. 2021. "Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods," *IEEE Access* (9), pp. 11895–11910.

Williams, E. J., Beardmore, A., and Joinson, A. N. 2017. "Individual Differences in Susceptibility to Online Influence: A Theoretical Review," *Computers in Human Behavior* (72), pp. 412–421.

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*.

Wright, R., Chakraborty, S., Basoglu, A., and Marett, K. 2010. "Where Did They Go Right? Understanding the Deception in Phishing Communications," *Group Decision and Negotiation* (19:4), pp. 391–416.

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

Wright, R. T., Johnson, S. L., and Kitchens, B. 2023. "Phishing Susceptibility in Context: A Multilevel Information Processings Perspective on Deception Detection," *MIS Quarterly,* 47(2).