Telematics and Informatics 67 (2022) 101766

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

The impact of formal and informal organizational norms on susceptibility to phishing: Combining survey and field experiment data

Gregor Petrič [a,*], Kai Roer [b]

[a] University of Ljubljana, Faculty of Social Sciences, Kardeljeva ploscad 5, SI-1000 Ljubljana, Slovenia
[b] KnowBe4 Research AS, Kristian Augustsgate, 13, Oslo, Norway

ARTICLE INFO

Keywords:
Information security
Norms
Phishing
Human factors
Social engineering
Organizational behavior

ABSTRACT

Phishing is one of the most common forms of social engineering that exploits human vulnerabilities and causes immense personal and organizational costs. This study advances the research on the factors of susceptibility to phishing in three regards. First, it addressed the role of organizational norms in susceptibility to phishing. Second, it aimed for high external and ecological validity by combining survey and phishing experiments data on large samples of organizations and their employees. Third, it employed a two-level design that considered explanatory variables at the individual and organizational levels. The study chiefly explored how formal, descriptive, injunctive, and personal norms influence employee interactions with phishing emails. To this end, an explanatory model was tested on 83,269 employees in 510 organizations using a multilevel modeling approach. Clicking on links in simulated phishing emails and entering personal information in simulated fraudulent websites were deemed as two types of susceptibility to phishing. Formal norms and collectively shared injunctive norms were found to exert the strongest effects on susceptibility to phishing; in contrast, personal norms exert a weak influence, and descriptive norms can result in a boomerang effect. These results have significant theoretical and practical implications for both researchers and managers seeking organizational-level mechanisms to reduce the threat of phishing emails.

1. Introduction

Email communication remains a leading online communication technology and an integral part of numerous organizational processes (Radicati, 2020; Wang et al., 2012), yet it is simultaneously a source of great vulnerability for organizations. Phishing emails, which take advantage of the human vulnerability to the biological principle of mimicry, are not entirely preventable (Aleroud and Zhou, 2017; Arachchilage and Love, 2014; Downs et al., 2006; Metalidou et al., 2014) and are the main cause of organizational security breaches. According to a recent Verizon data breach report, 25% of all security breaches involved phishing attacks (Bassett et al., 2020). Phishing is the most common type of social engineering attack that causes critical damage to organizations, ranging from identity theft and intellectual property theft to financial fraud, cyber espionage, operational problems, and reputational damage (Piggin, 2016). Phishing attacks have been targeting organizations since the late 1990s, and in the last two decades they have evolved

* Corresponding author.
E-mail addresses: gregor.petric@fdv.uni-lj.si (G. Petrič), kair@knowbe4.com (K. Roer).

https://doi.org/10.1016/j.tele.2021.101766
Received 8 January 2021; Received in revised form 7 December 2021; Accepted 17 December 2021
Available online 21 December 2021

into "powerful and dangerous cybersecurity weapons" (Taib et al., 2019, p. 581). With online processes becoming ubiquitous, especially due to the COVID-19 pandemic, it is not surprising that the number of phishing attacks doubled in 2020 alone (APWG, 2021). Continuous research of this critical problem for information security and organizations is thus essential.

Scientific and professional literature offers rich insights into the reasons some people are likely to fall prey to phishing emails, for example, by clicking a link that leads to a fraudulent website, opening an attachment with a malware code, or even offering their credentials on a fraudulent website. Several theoretical models have been developed and empirically tested that explain and offer evidence on how psychosocial, cognitive, and demographic factors result in susceptibility or resistance to phishing emails. Among them, the integrated information processing theory (Vishwanath et al., 2011) and the related suspicion, cognition, and automaticy model (Vishwanath et al., 2018), the application of the technology threat avoidance theory (Arachchilage and Love, 2014), and the application of the theory of deception (Wang et al., 2012) have the greatest explanatory power. In addition to the cited survey-based studies, a recent systematic review (Sommestad and Karlzén, 2019) of field experiments quite similarly showed that susceptibility to phishing is influenced primarily by suspicion-related variables, knowledge, message-level variables, and situational factors, such as high email load (Vishwanath et al., 2011) and general risky behavior on the internet (De Kimpe et al., 2018).

The present research was initiated by the observation that the current studies have three limitations. First, as the results of a recent systematic review (Sommestad and Karlzén, 2019) and a focus-group study (Williams et al., 2018) imply, research on susceptibility to phishing in the workplace should include a wider consideration of norms. Norms have recently been demonstrated as an important factor that determines compliance with information security policies (ISP) (Yazdanmehr and Wang, 2016) and can be subject to managerial decisions (Cialdini et al., 1999). Studying norms may reveal managerial mechanisms, besides the common approach of training, to fight susceptibility to phishing (Kumaraguru et al., 2009; Sheng et al., 2010). Second, the empirical tests of the above-mentioned psychosocial models of susceptibility to phishing often faced issues of external validity. This is because they were based on limited samples (students or a single organization) and low ecological validity due to measures of susceptibility that often do not measure actual behavior (Sommestad and Karlzén, 2019). Third, the studies overlooked that the percentage of people susceptible to phishing varies significantly among different cultures, organizations, and industries (Flores et al., 2015; Knowbe4, 2020), suggesting the use of a two-level research design, the most valid approach in cases where units (employees) are embedded in higher-level entities (organizations). Such a design, since social influence mechanisms seem to work differently in different work contexts, also seems relevant for substantive reasons (Williams et al., 2018). However, this type of design is rarely adopted: it demands sufficiently large samples of organizations and employees per organization.

The main research question is, thus, how different types of security-related organizational norms are associated with employees' actual phishing behavior? To explore this question, the study used a two-level research design on samples of organizations and their employees. Our large-scale study is, to our knowledge, the first to not only investigate an extremely large sample of employees ($n = 83{,}269$) from a large sample of organizations ($n = 510$) but is also based on merging the survey data on key explanatory variables of the research model with actual phishing data from field experiments.

The rest of this paper is organized as follows: we first provide a literature review of the three main theoretical pillars of our research model. Then we present the research model with hypotheses, the two-level research design that merges the survey and phishing experiments, and the results. Finally, we discuss our findings, implications, and limitations and conclude the paper.

2. Theoretical background

2.1. The psychosocial processes behind susceptibility to phishing

While phishing is defined as a social engineering crime—a so-called semantic attack (Arachchilage and Love, 2014) where an attacker sends a legitimate-looking email to persuade users to click on a link and reveal some personal information that is subsequently abused by the attacker (Vishwanath et al., 2011)—susceptibility to phishing in the workplace can be understood as an employee's tendency to interact with phishing emails in a way that puts organizational assets at risk. In other words, susceptibility to phishing refers to the likelihood of performing an action requested in a fraudulent message—such as clicking on a malicious link in an email, entering credentials and personal information on a phishing website, and downloading a malicious attachment that can secretly download and install ransomware or spyware (Chen et al., 2020; Harrison et al., 2015).

Behind this phenomenon is a complex mechanism involving the interactions of numerous psychosocial factors that result in a specific behavior when encountering a phishing email. One of the most notable and empirically supported mechanisms is delineated in the complementary information processing model of phishing (Vishwanath et al., 2011); the suspicion, cognition, and automaticity model (Vishwanath et al., 2018); and the applied theory of deception (Wang et al., 2012). According to the common premise, falling prey to a phishing email is largely dependent on how a person cognitively processes the email. Heuristic information processing—less cognitively resourceful and characterized by the habitual or automatic processing of email—will more likely result in being phished. Conversely, systematic information processing—a more elaborate, thorough, and "stop and think" processing of emails—has been empirically shown to significantly decrease the likelihood of being phished.

However, research has also shown that detecting suspicious email and acting on it is a complex, multistage process—starting from the initial raising of attention to generation of suspicion and its evaluation and assessment—a process that is not necessarily always successful (Chen et al., 2020). That is, even if an individual systematically processes fraudulent email, their decision-making process might still yield misjudgment, and they could fall into the trap (Chen et al., 2020).

A whole research stream has emerged from this baseline framework, which aims to identify the main factors behind the type of information processing and search for the initiators of thorough, systematic email processing. One important finding is that variables

that are central to the protection motivation theory (Bayl-Smith et al., 2021) and the related technology threat avoidance theory (Arachchilage and Love, 2014) are relevant in this context. Specifically, it has been demonstrated that when individuals expect their actions to have severe consequences, they are more likely to systematically process emails (Vishwanath et al., 2018). Further, a perceived threat motivates phishing threat avoidance behavior and, subsequently, leads to the actual avoidance of potential threats (Arachchilage and Love, 2014). Moreover, threat susceptibility, a recent study highlighted, lowers individuals' tendency to click on phishing links (Bayl-Smith et al., 2021).

An important question then, is this: Since email use is largely routinized and likely to be processed heuristically, how can employees be stimulated to systematically process emails? (Vishwanath et al., 2018). Enhancing user education and knowledge is a common answer, but in the workplace context, the possibility of intervening in organizational norms, we argue, should also be considered.

2.2. Organizational norms theory and social influence

Norms are invisible, supra-individual, and external "social facts" (Durkheim, 1895) that significantly impact human behavior. They are the generalized expectations of behavior in a certain social context and the "social glue" that facilitates cooperation and coordination among different social actors and enables smooth functioning of social groupings (Habermas, 1985). When a social norm is in force, members of society expect other members to behave in certain ways in given situations (Burnett et al., 2001). Such norms are sustained by feelings of embarrassment, anxiety, guilt, and shame that a person suffers at the prospect of violating them (Elster, 1989). The early researchers of social processes in organizations revealed how important social norms are in organizational contexts. In particular, Taylor (1911) explained that new, efficient employees are more likely to conform and become inefficient in a group of inefficient employees than vice versa—a newcomer becoming a motivator of change in a group of existing employees. Norms have also proven to be influential in various other contexts, and they have often been manipulated in social marketing and health campaigns to elicit positive behaviors.

We can differentiate between formal and informal organizational norms (Smith and Terry, 2013). For formal norms, researchers also use the term "rules," as they are formally codified in the guidelines and manuals that explicitly outline organizational rules. Informal norms, owing to their intersubjective existence, are also called social norms (Burnett and Bonnici, 2003); they are the "unwritten rules" not promulgated by an organizational authority but based on socially shared beliefs about what people ought to do, usually involving some sort of social sanction (Dequech, 2009; Smith and Terry, 2013). Since they are enforced by the approval or disapproval of other people in a group or community, they are informal, and they define the "normal" ways of handling things in an organization. This type of intersubjective sharing of acceptable and desired behaviors decisively impacts employee behaviors.

As Reno et al. (1993) and Rimal and Real (2003) suggested, within the category of informal norms, it is important to further distinguish between descriptive and injunctive norms. This distinction proves important not only for explaining how norms influence behavior but also for manipulating norms to achieve specific organizational or socially beneficial goals (Cialdini, 2009). *Descriptive norms* refer to the behaviors commonly exhibited in a certain context; they motivate actions by informing people about the behavior that is likely to be effective or adaptive in a certain context. They wield the power of informational influence (Deutsch and Gerard, 1955), where the prevalence of a certain behavior is considered the benchmark for the types of behavior that are accepted and desired (Rimal and Real, 2003). *Injunctive norms*, in contrast, refer to the peer approval or disapproval of certain behaviors; they influence behavior mainly through the social rewards and sanctions from engaging (or not engaging) in a certain behavior. Notably, as delineated in the theory of planned behavior (TPB), the concept of injunctive norms is equivalent to the concept of subjective norms (Ajzen, 1991). Though descriptive and injunctive norms are frequently interconnected, there is compelling evidence that they exert different influences on behavior. Moreover, there are often discrepancies between the two: although the majority of employees might perceive that important peers consider it inappropriate to write passwords on sticky notes (injunctive norm), the majority of employees still write passwords on sticky notes (descriptive norm).

Lastly, norms theory includes personal norms. They are internalized social norms (Kallgren et al., 2000; Rimal and Real, 2003), and since they are subconsciously absorbed by individuals and provide a moral orientation for action, they supposedly exert the strongest influence on behavior. Once internalized, behaving in line with the norm becomes something that is completely "normal" for the employees (Schwartz, 1977).

2.3. Norms in the security context

The field of behavioral information security recently applied Rimal's distinction between descriptive and injunctive norms (Wiafe et al., 2020; Yazdanmehr and Wang, 2016). In this context, descriptive norms pertain to the security compliance behaviors of others, while injunctive norms refer to the expectation of others to behave in accordance with an organization's ISP (Wiafe et al., 2020). In organizational settings, "others" refers to workplace peers, superiors, and managers (Herath & Rao, 2009). Security-related personal norms reflect individuals' commitment to their value system, which places (organizational) security among the top values, at least while acting in the organizational context (Yazdanmehr and Wang, 2016). The concept of formal norms is understood in terms of the rules and guidelines delineated in the ISP and how they are disseminated across the organization and materialized in a set of symbols, giving employees the formal guidelines for expected behavior (Shahbaznezhad et al., 2021).

Currently, investigations on how the different types of norms impact susceptibility to phishing are lacking. Studies have been focusing on how norms influence behavior in terms of compliance with ISP, yielding somewhat inconsistent results. But they have confirmed that descriptive and injunctive norms that support information security have, after controlling for numerous demographic and organizational variables, a weak to moderate direct (Yazdanmehr and Wang, 2016) or indirect (Wiafe et al., 2020) influence on

information security compliance. Further, descriptive norms and feelings of personal obligation lower resistance to information systems security (Merhi and Ahluwalia, 2019). The earlier studies that applied TPB, focused on subjective norms – which are equivalent to injunctive norms in the norms theory - demonstrated somewhat inconsistent results (Sommestad et al., 2013). The findings of most studies, however, suggest that subjective norms influence intentions to comply (Bulgurcu et al., 2010; Herath and Rao, 2009; Vance et al., 2012) and misuse (Guo et al., 2011) but do not directly influence actual compliance or misuse. All these studies, it must be noted, used self-reported measures of actual compliance and/or misuse.

3. Explanatory model and hypotheses

To address our central research question we applied the above distinction of the four types of norms. In the security context, we specified these norms as security-supportive norms, since they embrace the rules, behaviors, and expectations substantively related to organizational security. As Table 1 suggests, we introduced another often theoretically considered but rarely empirically investigated layer to differentiate the norms. This distinction relates to the ontological level in terms of understanding norms as individual- or organizational-level phenomena. As individual-level phenomena, they relate to perceived norms (what individuals think others think and how they behave), while at the organizational level, they pertain to norms as organizational characteristics that exist independently of the individual, in terms of predominant group behavior, collective expectations, and the salience and existence of formal norms (Hofstede, 2001; Schwartz, 1977). This distinction is relevant because studies have shown that perceptions may differ from common social norms (Hofstede, 2001), suggesting their different effects on behavior.

If we apply this distinction of norms to explain susceptibility to phishing, it seems logical that security-supportive personal norms will directly lower susceptibility to phishing. This is because, if we extrapolate Schwartz's (1977) argument, expectations of certain behaviors are internalized and guide how employees will interact with emails. Moreover, if we consider attitudes as manifestations of personal norms (Crandall et al., 2002; Mackie et al., 2015), the research that applied the TPB implies a positive association between personal norms and security-related behaviors (Bulgurcu et al., 2010; Flores and Ekstedt, 2016). It is thus safe to assume that if a person internalizes organizational security and considers taking care of security "normal," then it is likely that this person will be more careful, likely engage in systematic processing of emails, and, ultimately, be less likely to interact with phishing emails. Thus, our first hypothesis is as follows:

H_1. Security-supportive personal norms will lower susceptibility to phishing.

Descriptive norms are considered both as objective facts, in terms of how people generally behave in security-related organizational activities, and as employees' perceptions of what they think others are doing when interacting with organizational ICT. As descriptive norms have been demonstrated to impact ISP compliance (Yazdanmehr and Wang, 2016), a similar mechanism should arguably work in employees' handling of emails. When someone observes that others are careful in using the internet, talking about phishing emails, and exchanging experiences, it has an informational influence that sets a benchmark of what the rational behavior is in a certain situation. Moreover, if the majority of employees demonstrate behaviors resistant to phishing, this will also have a normative influence on individual employees: it will guide them by showing what the "right thing to do" is. To make efficient security-related decisions, employees will observe their coworkers' behavior and take it as the correct behavior to follow (Yazdanmehr and Wang, 2016). Thus, we hypothesized that descriptive norms, both on the individual and organizational level, will impact susceptibility to phishing.

H_{2a}. Perceived security-supportive descriptive norms will lower susceptibility to phishing.

H_{2b}. Objective security-supportive descriptive norms will lower susceptibility to phishing.

While arguing the impact of injunctive norms on susceptibility to phishing, it is also relevant to treat them at the individual and organizational levels. At the individual level, injunctive norms are equivalent to subjective norms (Fishbein and Ajzen 2011). Employees can recognize guidelines for their security-related behavior through their perception of what the majority of their coworkers expect. The mechanism for activating injunctive norms lies in social benefits or penalties (Rimal and Real, 2003). We suggest extrapolating this association to phishing and argue that if, for example, one believes that falling into the trap of a phishing scam will result in some social sanction, such as finger pointing, then we would expect that employees will be more attentive in their daily email

Table 1
Types of organizational norms depending on norms as individual- or organizational-level phenomena.

Type of norms / Ontological level	Individual-level phenomena	Organizational-level phenomena
Personal	Personal norm (moral obligation to carefully interact with ICT, follow the ISP, value organizational security)	/
Descriptive	Perceived descriptive norms (perception of how others interact with ICT, talk about security, handle emails, store passwords, etc.)	Objective descriptive norms (Dominant behaviors of others when interacting with ICT)
Injunctive	Perceived injunctive norm (perceived expectations of how one should interact with ICT, communicate, and value security)	Objective injunctive norms (Group's shared expectations of how one should interact with ICT)
Formal	Perceived formal norms (perception of existence and content of the ISP)	Objective formal norms (Existence of the ISP and their salience)

Note: Since personal norms only exist in the human mind and not as organizational characteristics, the above ontological distinction is not relevant for them.

routines to avoid this. Jacobson et al. (2020) similarly argued that because of the costs and benefits that arise with social sanctions and rewards from others, following injunctive norms tends to be associated with a more cognitively effortful decision-making style. This effort is characteristic of the systematic processing of information, thus resulting in lower susceptibility to phishing (Vishwanath et al., 2011; Vishwanath et al., 2018). Further, we can argue that the shared expectations in organizations, independent of individual perceptions, create an environment where it is normal to be suspicious and deviant to have a laissez-faire attitude. Such an environment will be beneficial for raising cyber-risk beliefs, which will stimulate the systematic processing of information, resulting in avoiding interaction with phishing emails (Vishwanath et al., 2018). We thus formulated the following hypotheses:

H_{3a}. Perceived security-supportive injunctive norms will lower susceptibility to phishing.

H_{3b}. Objective security-supportive injunctive norms will lower susceptibility to phishing.

Lastly, formal norms are understood as the existence and salience of organizational ISP on the one hand and the perceptions of these policies on the other hand. An organization's ISP defines a set of rules and policies regarding employee access to and use of organizational information assets, including the handling of emails (Alqahtani, 2017). As an ISP also describes the responsibilities of employees and the consequences of policy violations (Bulgurcu et al., 2010), we can assume that the existence and awareness of formal norms lead to the awareness of consequences, threat perception, and personal responsibility, which, according to signal detection theory (Canfield et al., 2016) and technology threat avoidance theory (Arachchilage and Love, 2014), will impact susceptibility to phishing. More specifically, formal norms help establish a belief that actions on the internet are risky, and there is empirical evidence that such a belief increases systematic information processing, which increases the possibility of phishing resistance (Vishwanath et al., 2018). It is not enough for formal norms to exist—they must be made salient by proper communication and acknowledged by employees (Merhi and Ahluwalia, 2019). Strong leadership that would enable this has been shown to indirectly impact the intention to resist phishing (Flores and Ekstedt, 2016). We thus derived the following hypotheses:

H_{4a}. Perceived security-supportive formal norms will lower susceptibility to phishing.

H_{4b}. Objective security-supportive formal norms will lower susceptibility to phishing.

Having delineated these hypotheses, it must be noted that our study was limited from the outset in terms of the variables and items we could measure (in terms of cooperation with the company that provided the platform for collecting and supplying data). Consequently, we focused solely on explaining the direct influences of the different types of norms on susceptibility to phishing, as these are the most relevant in potential managerial implications. We thus avoided testing the hypotheses that would link norms with psychosocial processes and susceptibility to phishing. We were also unable to consider some organizational characteristics that likely interact with the impact of norms, such as organizational climate and sense of belonging.

4. Methodology

4.1. Participants and data collection

To test the hypotheses, we implemented a two-level research design, mixing survey and phishing experiments data. The study was conducted in collaboration with KnowBe4 Research AS, the global research unit of the US-based company KnowBe4 that offers products in security awareness, behavior, and culture space. Two of its products were relevant for this research (see Fig. 1): a survey on the human factors of security including items on norms, which our research team provided, and a phishing campaign including a series of phishing experiments, where the employees of a customer organization occasionally received unannounced simulated phishing emails. The customer organization could decide which product to activate. Once the survey was activated, all the employees received an invitation to complete the survey, or once the phishing experiment product was activated, all the employees got involved in a simulated phishing campaign. In collaboration with the company, we received the relevant, anonymized data from the survey and the phishing campaigns. The data were merged into a single dataset with a unique ID for each employee and each customer organization. In other words, the dataset provided information concerning the norms items from the survey, the data on each employee's actions with phishing links, and the ID of the organization to which the employees belonged.

At the time of this study, the company had more than 35,000 customers (organizations) worldwide. We received an anonymized dataset for a sample of US-based organizations. The sample was limited to organizations that started with phishing experiments no earlier than January 1, 2019, and conducted one human factors survey on employees during a period of 1.5 years between January 1,

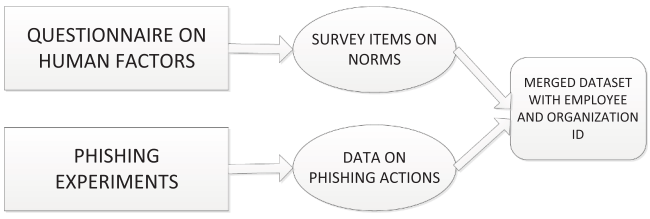

Fig. 1. Two sources of data.

Table 2
Numbers of employees and organizations according to organizational size.

	Total	Small and Medium org. (up to 250 employees)	Large org. (250 employees and more)
No. of employees	83,269	19,941	63,328
No. of organizations	510	339	171
Mean (no. of employees per organization)	621.3	101.9	1,650.9
SD (no. of employees per organization)	3,563.4	61.3	6,033.8

2019, and June 30, 2020. After excluding the organizations with a survey response rate below 25% and fewer than 20 valid employee responses, the final sample consisted of 510 organizations with 83,269 employees. Table 2 shows the average number of employees per organization, separated into two organizational sizes. The average size of the organizations was 621.3 employees, but this varied considerably (SD = 3,563.4). Our sample included more small organizations with up to 250 employees (n = 339) and fewer organizations with more than 250 employees (n = 171).

The sample, it must be noted, was not random; some relevant control variables, such as socio-demographics and year of employment, are missing. However, as explained already, we were extremely limited in the number of items to be included in the survey. Further, although we could not control accurately for security awareness trainings, our analysis was limited to similar organizations, in the sense that these companies started their security awareness programs in 2019 and, thus, had some minimum security training in place.

4.2. Measures

4.2.1. Field experiment measures of susceptibility to phishing

Susceptibility to phishing is usually measured via one of the three approaches: survey questions that measure self-reported behavior (i.e., Bulgurcu et al., 2010), role-play scenarios within a survey (i.e., Sheng et al., 2010), and phishing experiments or "drill-style" studies (Flores and Ekstedt, 2016; Jalali et al., 2020; Sommestad and Karlzén, 2019). We undertook the latter approach, where the employees received simulated phishing emails and the company's software system monitored their responses. The recordings of actual employee reactions to simulated phishing emails are arguably the most valid measure of susceptibility to phishing (Sommestad and Karlzén, 2019; Taib et al., 2019).

Employees from the 510 sampled companies received a variable, unannounced number of simulated phishing emails over a period of 1.5 years, and the system recorded the varied actions the employees took in response to the received emails, including whether they clicked on the link on a fraudulent website and whether they entered their personal data. Though the system also recorded additional actions such as opening and reporting phishing emails, this study did not focus on them.

As Chen et al. (2020) argued, most studies have focused on a single, event-specific phishing susceptibility and not across a series of phishing emails. In this context, it is important to distinguish between employees who never failed a phishing experiment and those who fell into the trap of a phishing email at least once—subsequent encounters with phishing incorporate the experiences of previous encounters (Chen et al., 2020). The methodological implication is that susceptibility to phishing in our study was treated as two different variables (see Table 3): resilience to phishing, a nominal variable that distinguishes between those who were never phished and those who got phished at least once, and frequency of phishing failures, an interval variable computed only for those who were phished at least once.

Considering this premise and the different actions the employees undertook when confronted with phishing emails, our study delineated four dependent variables, as shown in Table 3. For the subsample of employees who failed in at least one phishing campaign, the average percentages of the clicking and data entry were calculated. These two variables, thus, had theoretical scale on interval [>0% – 100%]. A smaller number represented an employee who typically infrequently clicked on links or entered data in phishing emails. Therefore, if an employee had a value of 100% for the "clicking" variable, this meant he/she clicked on the links in all the phishing emails he/she received. Conversely, an employee with a value of 10% for the "data entry" variable entered personal information on simulated fraudulent websites in, on average, 1 out of 10 phishing emails.

Since people receiving more phishing emails are at a higher risk of becoming victims, we treated the information about the number of phishing emails received by each individual as a control variable (De Kimpe et al., 2018) in the models that aim to explain frequency of phishing failures.

4.2.2. Survey-based measures of norms

The measurement instruments for norms were part of the collaborating company's survey on the human factors of information security (see Fig. 1). Our research team provided the items for measuring the different types of norms, and they were inserted in the survey module offered to the company's customers. The measures were developed according to DeVellis (2003) standard prescriptions. The items were based on the essential definitions of each type of norm and derived from previously validated measures of security-related norms in the literature. The scale for personal norms was adopted from Safa et al. (2015) and Yazdanmehr and Wang

Table 3
Dependent variables in the study and their values.

Phishing action/ Situation	Resilience to phishing (Never failed vs. failed at least once)	Frequency of failure (Average percentage of failures in a sample of those who failed at least once)
Clicking links	Clicked on at least one email = yes (1) or no (0)	Average clicking % = Number of clicks / Number of all phishing emails*100
Entering data	Provided data in at least one email = yes (1) or no (0)	Average data entry % = Number of data entries / Number of all phishing emails*100

(2016) and reflected the extent to which an employee internalizes security-related norms and related behaviors as a normal way of thinking and doing in an organization (sample item[1]: "I feel morally obliged to support the organization's security decisions, like blocking access to some websites"). The measures for information security-related descriptive and injunctive norms were derived from Rimal and Real (2003) and Yazdanmehr and Wang (2016). The descriptive norms items (sample item: "In our organization, people store passwords in visible places in their office" [reversed item]) reflect the employee's observation of how their coworkers understand and behave when using organizational IT devices, while the items of injunctive norms represent the social pressure, approval, and disapproval from coworkers regarding certain security-related behaviors and attitudes (sample item: "My coworkers expect that I will take great care when dealing with confidential information"). The measurement instrument for formal norms was developed following Cooke and Szumal (1993), Da Veiga and Martins (2015), and Flores and Ekstedt (2016) and grasps the extent to which the employees perceive the existence of ISPs and their content and clarity (sample item: "I'm well informed about the content of information security policies of our organization"). All the items were measured on a five-point Likert-type scale of agreement.

In 2016, our research team designed an extensive initial pool of items that was subjected to an expert review and pilot study. First, three experts from the fields of social science methodology, information security, and social psychology judged the items for relevance and clarity. After obtaining their feedback, the items were optimized and applied to a pilot study to test the quality of measures in terms of validity and reliability and to identify a smaller, parsimonious set of items. The pilot study was run on a sample of 110 employees of two Norwegian educational organizations. Exploratory and confirmatory factor analyses were used to confirm the four-factor structure of the norms measurement instrument. Based on the open answers in the pilot study, we optimized some items and made them more intelligible. As we were instructed by the collaborating company to minimize the number of items, factor analyses were used to exclude redundant items (Anderson and Gerbing, 1991) and identify a parsimonious set of items, resulting in 15 items for the norms measurement instrument (see Table 4).

The measurement model was tested using multi-level confirmatory factor analysis (package lavaan in R) to examine the different facets of reliability and validity. To inspect reliability, Cronbach's alpha was assessed, where the value needed to be above 0.7 to be accepted, or above 0.6 in the case of a small number of items (Loewenthal and Lewis, 2015). We also inspected the fit of the proposed factor model as well as convergent and discriminant validity, which was based on the following typically used logic (Hair et al., 2014): the square root of the average variance extracted (AVE) from a single measure should be higher than its correlations with other measures. Note that the reliabilities of individual-level measures for norms were comparably lower than those in other studies. This could relate to the fact that, in developing our items, we wanted to avoid the general wording of "information security"—respondents, our pilot study suggested, find this word too vague and might provide socially desirable responses (Lebek et al., 2014). Our solution was to include concrete illustrations of security-related issues, such as handling emails, passwords, and sensitive data, but the downside to this could be that involvement in such activities does not necessarily correlate with other activities within the same factor, thus resulting in lower individual-level correlations.

The measurement model demonstrated a good fit to the data (χ^2 = 1,094.5; df = 165; CFI = 0.90, TLI = 0.87, SRMRb = 0.056, SRMRw = 0.033). The factorial weights and Cronbach's alpha also pointed to good internal consistency of all measurement instruments, except the scale of personal norms at the individual level, which had marginal reliability. For other types of norms, the measurement instruments had better reliability at the organizational level. All the measurement instruments demonstrated satisfactory discriminant and convergent validity (see Table 5). All the variables were then computed as arithmetic means of the corresponding items. The organizational-level descriptive, injunctive, and formal norms were computed as aggregations of the individual-level responses on particular items and then summed into composite variables. Taking these aggregations as surrogates of the actual norms present in an organization is a sufficiently valid technique (Peterson and Castro, 2006).

4.3. Hypothesis testing methods

To test the hypotheses, we used the multi-level modeling approach (Hox et al., 2017; Snijders and Bosker, 2011) suitable for situations where first-level units (employees) are nested within second-level units (organizations), thus assuming some dependence between first-level units. The choice of a multilevel approach was also empirically justified because the intra-class correlation coefficient for the dependent variables ranged from 0.29 to 0.55, suggesting that from 29% to 55% of variability in susceptibility to phishing was attributable to organizational-level factors. These numbers greatly exceeded the suggested threshold value of 0.1 for the intra-class correlation coefficient (Hox et al., 2017).

[1] For intellectual property reasons, we cannot disclose the exact wordings of items, but we provide somewhat modified sample items for each concept.

Table 4
List of all items, factorial weights, Cronbach's alpha values, and average variance extracted (AVE).

Latent construct	Item	Factor loading (individual/ organizational level)	Cronbach's alpha (individual/ organizational level)	AVE (individual/ organizational level)
Security-related personal norms	Pnorm1	0.60	0.61	0.25
	Pnorm2	0.37		
	Pnorm3	0.48		
	Pnorm4	0.44		
	Pnorm5	0.58		
Security-related descriptive norms	Dnorm1	0.89/0.99	0.77/0.83	0.54/0.63
	Dnorm2	0.44/0.60		
	Dnorm3	0.79/0.74		
Security-related injunctive norms	Inorm1	0.81/0.92	0.71/0.85	0.50/0.72
	Inorm2	0.52/0.69		
	Inorm3	0.76/0.91		
Security-related formal norms	Fnorm1	0.64/0.84	0.75/0.94	0.49/0.83
	Fnorm2	0.75/0.94		
	Fnorm3	0.62/0.91		
	Fnorm4	0.77/0.94		

Table 5
Construct correlations (individual and organizational level).

	Personal norms	Descriptive norms	Injunctive norms	Formal norms
Personal norms	0.5			
Descriptive norms	0.32	0.73/0.79		
Injunctive norms	0.46	0.42/0.76	0.71/0.85	
Formal norms	0.48	0.30/0.54	0.51/0.69	0.70/0.91

Note: The diagonal represents the square root of AVE values.

According to our differentiation of the dependent variables (see Table 3), we ran logistic multi-level regression (package glmer in R) for the model where the dependent variable was of a nominal type (resilience to phishing) and ordinary multilevel regression (package lmer in R) where the dependent variable was of an interval type (frequency of phishing failures).

To inspect the stability of the model and control for company size, we ran each model for the whole sample and also separately for small and medium companies (SMOs; up to 250 employees) and large companies (more than 250 employees).

To test the fit of the model, we considered different fit indices. For the multilevel logistic regression model, we computed the difference in log likelihood and the value and significance of area under curve (AUC); for the ordinary multilevel regression, we studied the significance of the increase in R^2 and the absolute value of R^2 (Hox et al., 2017).

5. Results

5.1. Descriptive analysis

The basic descriptive statistics of all the variables in the model for the whole sample and separately for the two categories of organizations are presented in Table 6.

In the sample, 34.7% of employees clicked on a link in a phishing email at least once, while 4.9% entered data in a simulated phishing website at least once. We found significant differences in susceptibility to phishing depending on the size of the organization.

Table 6
Descriptive statistics of variables in the model (mean % and standard deviation).

Variable	Total sample	Small & medium organizations	Large org.	Difference SMO vs. large (P-value)
Clicked on link in at least one email	34.7% (47.6)	37.9% (48.5)	33.2% (47.1)	< 0.005
Entered data in at least one email	4.9% (21.6)	4.5% (20.1)	5.1% (22.0)	< 0.005
Average percentage of clicks on links in phishing emails	34.5 (28.6)	24.0 (24.3)	40.2 (29.1)	< 0.005
Average percentage of entering data on phishing sites	31.3 (25.0)	25.2 (27.2)	33.8 (23.5)	< 0.005
Total number of phishing emails	6.6 (9.2)	12.1 (14.4)	4.8 (5.7)	< 0.005
Personal norms	4.04 (0.53)	4.11 (0.51)	4.02 (0.54)	< 0.005
Perceived descriptive norms	3.57 (0.80)	3.52 (0.81)	3.59 (0.80)	< 0.005
Perceived injunctive norms	3.93 (0.61)	3.95 (0.60)	3.92 (0.63)	< 0.005
Perceived formal norms	3.88 (0.66)	3.89 (0.68)	3.87 (0.65)	<0.005
Descriptive norms	3.56 (0.27)	3.57 (0.29)	3.56 (0.24)	n.s.
Injunctive norms	3.94 (0.19)	3.96 (0.21)	3.93 (0.17)	<0.005
Formal norms	3.89 (0.27)	3.90 (0.30)	3.88 (0.22)	n.s.

For example, the employees of SMOs were more likely to click on at least one phishing email but less likely to enter data in a fraudulent website than employees of large organizations. Regarding the frequency of phishing activities, the average percentages were significantly lower in SMOs. Namely, while the employees of SMOs, on average, clicked on the links in 24% of the phishing emails they received, the employees of large organizations clicked on the links in 40.2% of the phishing emails.

The differences between the organizations in terms of security-related norms are much smaller. However, due to the large samples of both employees and organizations, the differences are significant in most cases. The results suggest that SMOs have slightly better-developed security-supportive norms compared to large organizations. In general, all the organizations demonstrate quite well-developed norms of all types that support information security. The least developed norms appear to be the descriptive ones ($M = 3.56$, $SD = 0.27$).

5.2. Hypotheses testing

The hypothesis testing was divided according to the four different dependent variables (see Table 3) describing the specific aspects of susceptibility to phishing. Moreover, to explore the stability of the model, we examined whether it behaved in the same way for the two types of organizations.

Multilevel logistic regression analyses were run separately for clicking on phishing links and entering data in fraudulent websites. First, we report the results for the model in explaining resilience to clicking on links in phishing emails (see Table 7). The significant value of $-2LL$ ($-2LL = 80.5$, $P < 0.005$) statistics indicates that the model with predictors significantly better fits the data than intercept-only model. The significant value of the AUC statistics ($AUC = 0.733$, $P < 0.005$) indicates the model's good discriminating power (Hosmer et al, 2013). According to the values of the regression parameter estimates, a significant fixed effect of personal norms ($b = -0.07$), perceived injunctive norms ($b = -0.07$), formal norms ($b = 0.53$), and injunctive norms ($b = -1.07$) can be observed. Notably, the odds of susceptibility to phishing decrease by a factor of 0.34 if injunctive norms increase by one unit. In other words, resilience increases by a factor of 2.94. If personal norms increase by one unit, the odds of susceptibility decrease by 0.93. The same holds for perceived injunctive norms. Formal norms demonstrate the opposite effect as expected: an increase in security-supportive formal norms will also increase the likelihood of clicking by a factor of 1.7. The odds of susceptibility to phishing significantly decrease with an increase in personal norms for both types of organizations. In general, we can see consistent results across the two types of organizations, except for the impact of organizational-level norms, which becomes non-significant for large organizations. The R^2 values are, in all cases, small, indicating the rather weak explanatory power of the proposed model.

The model for resilience to providing data on fraudulent websites (see Table 8) also demonstrated a significant value of $-2LL$ ($-2LL = 49.2$, $P < 0.005$) and a significant yet not very high value of AUC statistics (0.61), suggesting the model's satisfactory discriminating power. At the individual level, we can observe that only perceived formal norms have a significant influence on resilience to providing data ($b = -0.07$, $P = 0.03$), suggesting that with an increase of perceived formal norms, susceptibility to phishing will decrease by a factor of 0.93. A stronger effect is noted for large organizations, where an increase in perceived formal norms will decrease the odds of susceptibility to phishing by a factor of 0.79 ($b = -0.24$, $P = 0.09$). Larger effects can be observed for organizational-level norms, as an increase in the salience of formal norms will decrease susceptibility to phishing by a factor of 0.24 ($b = -1.43$, $P = 0.03$). In large organizations, an increase in descriptive norms will significantly decrease susceptibility to phishing by a factor of 0.12 ($b = -2.10$, $P = 0.03$).

The frequency of phishing failures was examined with a series of multilevel linear regression models. Table 9 reports the results of the frequency of clicking on phishing links as the dependent variable. Comparing the model with all the predictors and the model with only the control variable (no. of emails) revealed a significant increase in R^2 ($P < 0.005$), suggesting that norm-related predictors in the model exert a significant effect on the dependent variable. The R^2 statistics show that the proposed model explains approximately 17% of the variability of clicking on phishing links. More precisely, it can be observed that all the variables have a statistically significant effect on frequency of clicking on phishing links. However, this effect is rather weak for individual-level variables. With an increase in personal norms ($b = -0.85$, $P < 0.005$), perceived formal norms ($b = -0.47$, $P < 0.005$), and perceived injunctive norms ($b = -0.76$, $P < 0.001$), there will be a decrease in susceptibility to phishing. There is an unexpected positive association between perceived descriptive norms and the dependent variable ($b = 0.58$, $P < 0.005$). A similar association is also present at the organizational level, as with an increase in security-supportive descriptive norms, susceptibility to phishing will increase ($b = 11.56$, $P < 0.005$). Formal norms

Table 7
Results of multilevel logistic regression with dependent variable "resilience to clicking on links in phishing emails"

	TOTAL			SMO			Large		
	Estimate	Odds Ratio	P-value	Estimate	Odds Ratio	P-value	Estimate	Odds Ratio	P-value
Personal norms	−0.07	0.93	<0.005	−0.14	0.87	<0.005	−0.06	0.95	<0.005
Perceived formal norms	−0.01	0.99	n.s.	0.02	1.02	n.s.	−0.01	0.99	n.s.
Perceived descriptive norms	0.01	1.01	n.s.	0.03	1.03	n.s.	0.001	1.001	n.s.
Perceived injunctive norms	−0.07	0.93	<0.005	−0.09	0.91	<0.005	−0.06	0.94	<0.005
Formal norms	0.53	1.70	0.04	0.66	1.93	0.03	0.35	1.42	n.s.
Descriptive norms	0.19	1.21	n.s.	0.09	1.09	n.s.	0.23	1.26	n.s.
Injunctive norms	−1.07	0.34	<0.005	−1.23	0.29	<0.005	−0.84	0.43	n.s.
R^2	0.04			0.06			0.05		

Table 8
Results of multilevel logistic regression with dependent variable "resilience to providing data on fraudulent websites"

	TOTAL			SME			Large		
	Estimate	Odds Ratio	P-value	Estimate	Odds Ratio	P-value	Estimate	Odds Ratio	P-value
Personal norms	0.22	1.25	n.s.	0.18	1.19	n.s.	0.22	1.25	n.s.
Perceived formal norms	−0.07	0.93	0.03	−0.01	0.99	n.s.	−0.24	0.79	0.09
Perceived descriptive norms	−0.02	0.98	n.s.	0.03	1.03	n.s.	−0.01	0.99	n.s.
Perceived injunctive norms	−0.09	0.91	n.s.	−0.09	0.91	n.s.	−0.02	0.98	n.s.
Formal norms	−1.43	0.24	0.03	−1.57	0.21	0.04	−2.60	0.07	0.02
Descriptive norms	−1.03	0.36	n.s.	−0.61	0.54	n.s.	−2.10	0.12	0.03
Injunctive norms	−0.53	0.59	n.s.	−0.65	0.52	n.s.	1.48	4.39	n.s.
R^2	0.03			0.04			0.03		

Table 9
Results of multilevel linear regression with dependent variable "frequency of clicking on phishing links "

	TOTAL			SMO			Large		
	Fixed effect	Standardized fixed effect	P-value	Fixed effect	Standardized fixed effect	P-value	Fixed effect	Standardized fixed effect	P-value
No. of emails	−9.74	−0.34	<0.005	−7.31	−0.30	<0.005	−9.8	−0.34	< 0.01
Personal norms	−0.85	−0.02	<0.005	−0.98	−0.02	<0.005	−0.83	−0.02	< 0.01
Perceived formal norms	−0.47	−0.01	<0.005	−0.36	−0.01	n.s.	−0.52	−0.01	< 0.01
Perceived descriptive norms	0.58	0.02	<0.005	0.32	0.01	n.s.	0.58	0.02	< 0.01
Perceived injunctive norms	−0.76	−0.02	<0.005	−1.06	−0.03	<0.005	−0.79	−0.02	< 0.01
Formal norms	−11.93	−0.10	<0.005	−19.86	−0.22	<0.005	−16.76	−0.12	0.01
Descriptive norms	11.56	0.11	<0.005	12.78	0.14	<0.005	14.74	0.14	< 0.01
Injunctive norms	−12.57	−0.08	0.09	−7.06	−0.05	n.s.	−11.33	−0.06	n.s.
R^2	17.0%			17.4%			17.2%		

(b = −11.93, P < 0.005) and injunctive norms (b = −12.57, P = 0.09) will decrease the frequency of clicking on phishing links, but for the latter, the effect is marginally significant. The associations are consistent across organization types, but we can notice that the effects of perceived formal and descriptive norms become insignificant in the case of SMOs.

The model explaining the frequency of providing data on fraudulent websites (see Table 10) has a statistically significantly better fit to the data than the model with only the control variable (P < 0.005). The proportion of the explained variance is 0.26, suggesting the model's good explanatory power, but a lot of the variability can be attributed to the control variable, indicating that the more phishing emails an employee is exposed to, the higher the frequency of being phished (b = −11.6, P < 0.005). Among the individual-level

Table 10
Results of multilevel linear regression with dependent variable "frequency of providing data on fraudulent websites"

	TOTAL			SME			Large		
	Fixed effect	Standardized fixed effect	P-value	Fixed effect	Standardized fixed effect	P-value	Fixed effect	Standardized fixed effect	P-value
No. of emails	−11.6	−0.46	<0.005	−14.3	−0.52	<0.005	−11.72	−0.46	<0.005
Personal norms	−0.04	−0.002	n.s.	−0.19	−0.01	n.s.	0.02	0.001	n.s.
Perceived formal norms	−0.11	−0.004	n.s.	−0.12	−0.01	n.s.	−0.04	−0.001	n.s.
Perceived descriptive norms	0.35	0.01	0.07	0.13	0.004	n.s.	0.33	0.01	0.08
Perceived injunctive norms	−0.64	−0.02	0.02	−0.27	−0.01	n.s.	−0.65	−0.02	0.02
Formal norms	−18.32	−0.15	0.02	−17.02	−0.17	0.03	−24.02	−0.19	0.02
Descriptive norms	12.69	0.11	n.s.	14.10	0.14	0.09	6.20	0.05	n.s.
Injunctive norms	−1.41	−0.01	n.s.	−8.40	−0.06	n.s.	10.28	0.06	n.s.
R^2	0.26			0.39			0.25		

variables, only perceived injunctive norms (b = −0.64, P = 0.02) have the expected significant effect, while perceived descriptive norms have a marginally significant but contrary to the expected effect (b = 0.35, P = 0.07). Among the organizational-level norms, formal norms significantly decrease susceptibility to phishing (b = −18.32, P = 0.02), while descriptive norms marginally significantly increase susceptibility to phishing (b = 14.10, P = 0.09) but only in SMOs. Injunctive norms do not demonstrate an effect on the frequency of providing data on phishing websites.

To conclude this section, Table 11 summarizes the hypotheses tests across different conditions, with three notable points. In line with the different understandings of susceptibility to phishing, the hypotheses were separately tested for nominal variable (resilience to phishing) and interval variable (frequency of phishing failures). Moreover, the hypotheses were tested separately for two types of phishing actions: clicking and providing data. We did not include the test across organization types, as the results demonstrate that the model is largely independent of organization size.

6. Discussion

6.1. Principal findings

This study chiefly aimed to investigate the influence of different types of norms—both as perceptions and organizational characteristics—on susceptibility to phishing. While most studies combining survey and phishing data have focused on a single phishing experiment, this study collected its data from a series of phishing experiments conducted over 1.5 years. Thus, the results are not directly comparable, yet our study reveals the rather worrying statistic that more than one third of employees clicked on a link in at least one phishing email. In single-event studies, this number is around 10% (Flores et al., 2015; Jalali et al., 2020). Notably, employees from 510 organizations were much less likely to enter personal data in a fraudulent website, activated by clicking the phishing link. Although 95.1% of employees never provided any personal data on a simulated phishing website, those 4.9% who fell into the trap at least once provided data quite frequently—in 31.1% of all phishing emails. In other words, those who are likely to be deceived will be deceived into providing sensitive data on every third phishing email. In this light, one important suggestion for further studies is to specifically investigate such a population of "repeate clickers" (Canham et al., 2021).

Regarding our research model, we found partial support for the impact of the three types of norms on susceptibility to phishing but not for descriptive norms (see Table 11). The (weak) impact of personal norms was present for clicking but not for providing data. The internalization of security-supportive organizational norms makes employees more resistant to clicking on links in emails, and they less frequently click on links, yet their moral commitment is not strong enough to avoid falling into the trap of fraudulent websites. The commitment to organizational security likely activates the systematic processing of emails (Vishwanath et al., 2018), yet this activation happens only in the pre-click phase, when an email is processed on the basis of visceral and deception triggers (Wang et al., 2012). After failing to detect phishing email in the pre-click phase, it is unlikely that an employee will detect deception in the post-click phase. Moreover, even when an employee becomes suspicious about a certain email or website, the detection decision process might result in non-detection (Chen et al., 2020). Another explanation could be that the moral commitment to organizational security might be too general and not interpreted as relevant for a specific situation, such as a phishing email (Yazdanmehr and Wang, 2016).

Formal norms decrease susceptibility to phishing both at the individual and organizational levels. Employees who perceive the existence of an ISP and understand it will be more likely to never provide data on fraudulent websites and less frequently click on links in phishing emails. The impact of formal norms as organizational-level phenomena is stronger than their perception. A salient and clearly communicated ISP will result in stronger resilience to providing data on fraudulent websites and reduced frequency of clicking on phishing links and providing personal data. A salient ISP likely helps in building awareness of risk threat and communicates the serious consequences of negligent behavior to employees, which evidently leads to lower susceptibility (Vishwanath et al., 2018). The effect of formal norms was, however, not consistent across all conditions, which is not unexpected, considering the empirical absence of influence of security policy awareness on phishing behavior in other studies that combined survey and phishing experiments (Flores et al., 2015).

Contrary to our expectation, an inverse association was found for the impact of objective formal norms on resilience to clicking.

Table 11
Results of hypothesis testing.

		Resilience		Freq. of failure		Result
	Hypothesis	Clicking	Data entry	Clicking	Data entry	
H_1	Personal norms → Susceptibility to phishing	✓	×	✓	×	Partial support
H_{2a}	Perceived descriptive norms → Susceptibility to phishing	×	×	↕	↕	Not supported
H_{2b}	Descriptive norms → Susceptibility to phishing	×	×	↕	×	Not supported
H_{3a}	Perceived injunctive norms → Susceptibility to phishing	✓	×	✓	✓	Partial support
H_{3b}	Injunctive norms → Susceptibility to phishing	✓	×	✓	×	Partial support
H_{4a}	Perceived formal norms → Susceptibility to phishing	×	✓	✓	×	Partial support
H_{4b}	Formal norms → Susceptibility to phishing	↕	✓	✓	✓	Partial support

Note:
✓ accepted.
× rejected.
↕ inverse effect.

Employees in organizations with clear and salient ISP will be more likely to click at least once on a link in a phishing email. This is not an entirely surprising finding; this phenomenon is known in other fields that investigate the impact of norms on behavior as a "boomerang effect" (Byrne and Hart, 2009; Schultz et al., 2007). Following researchers' argument about this effect, it is likely that a clear and salient ISP makes employees trust that the organization and system take great care of organizational security; consequently, they might think they do not need to bother with security issues. Note, however, that this association only happened with resilience to clicking and not with entering data in fraudulent websites, which is a much more serious security threat. Another explanation could be that there is some sort of subversiveness, identified in some previous studies as a consequence of (overly) heavy regulations, resulting in non-compliant behavior due to the rejection of ISPs (Merhi and Ahluwalia, 2019; Williams et al., 2018). However, this would need to be empirically verified by considering other relevant variables.

Perceived injunctive norms had a significant but weak direct influence on all perspectives of susceptibility to phishing except for resilience to data entry. What others think and expect from an employee plays a role in employee resilience to clicking on links and on the frequency of both phishing actions. One could speculate why other people's expectations and, with this, the connected social rewards more likely impact clicking than entering data. Namely, the employees might discuss the kinds of websites they encountered when clicking on phishing links, and deviating from expectations might generate feelings of embarrassment. Yet, discussions on how employees entered data in fraudulent websites are less likely to happen. In any case, it must be noted that the direct effect of injunctive norms was rather weak, which is not surprising—other studies have revealed that such norms indirectly affect behavior by changing attitudes and intentions toward behavior (Merhi and Ahluwalia, 2019). Our study revealed stronger direct effects of objective injunctive norms, which pertain to the shared expectations and rewards regarding employees' security-related behavior. Organizations where employees have strong, shared expectations about their peers' behavior establish a moral climate with strong awareness of both social and security-related consequences. This awareness of consequences increases the possibility of systematic processing of emails, making the detection of deceptive emails more likely (Vishwanath et al., 2018). As explained above, this process seems to work in the pre-click phase of processing the email but not in the post-click phase of interacting with a fraudulent website. This, however, is a speculation that demands empirical verification.

Regarding the impact of descriptive norms, none of the hypotheses were supported. The security-related behaviors of others, our results suggest, do not exert enough of a normative and informational influence (Deutsch and Gerard, 1955) to lower the susceptibility to phishing. A similar lack of power of descriptive norms was identified in recent studies on compliant behavior (Yazdanmehr and Wang, 2016). The absence of an expected association could also be attributed to the relative invisibility of behaviors such as interacting with emails to other coworkers. While no impact was found on resilience to phishing, the results, nevertheless, illustrate that the influence of descriptive norms on frequency of phishing failures is contrary to what was hypothesized. If the predominant behaviors of others are security supportive and employees perceive this as such, the employees will be less careful and more frequently fall victim to phishing, both in terms of clicking on links and entering data in fraudulent websites. This, we could speculate, is like the aforementioned boomerang effect or even more so like the free-rider effect in online communities (Beenen et al., 2004). Namely, employees might wonder why they need to care about security if enough coworkers are already taking care of it. Moreover, when employees see others strictly following security protocols, this leads to reduced perceived vulnerability to online threats, resulting in less secure behavior (Conway et al., 2017). This finding implies the importance of constantly advertising the responsibilities of each employee in the organization.

6.2. *Practical implications*

The results of our empirical study have direct implications for managers striving to suppress social engineering threats. To address the human aspect of the phishing problem, though organizations have taken important steps by providing training to educate employees, these efforts remain insufficient (Jalali et al., 2020). Since decision-makers can directly influence norms, we believe that focusing on norms opens an important aspect of researching and preventing phishing. Organizational norms, our findings reveal, can influence employees' behavior without necessarily persuading them directly. This is good news for management: External norms should be easier to control than individual-level processes, which are dependent on many factors and usually under the minimal control of the organization. This is one important attribute of norms compared to training: while training can be an effective persuasive technique, it is often a challenge to change employees' knowledge, personalities, and attitudes. In contrast, an organization's normative framework is much more malleable. Specifically, as norms are constructed, understood, and disseminated across the organization primarily through communicative processes (Rimal and Real, 2003), it should be quite straightforward for managers to intervene in these processes.

As Smith and Terry (2013) suggested, managers must assess and understand the organization's normative climate before trying to change employee behavior. If organizational norms regarding security are not considered, then security-related initiatives might fail to succeed, as employees resist change that is inconsistent with their understanding of appropriate behavior. Managers not only need to focus on how the ISP is codified but also how it is disseminated across the organization and communicated among employees. Establishing a greater awareness of consequences through formal norms could result in the systematic processing of emails that decreases susceptibility to phishing. Moreover, to avoid the boomerang effect, individual responsibilities must be highlighted through injunctive norms. Injunctive norms are intersubjective, but managers can influence them through various organizational actions, where expectations regarding employee behavior are subtly communicated. Managers must move beyond general messages (Canfield et al., 2016) to specific messages about expectations regarding interactions with emails in the form of visible material—such as posters placed at meeting places in the organization—through which injunctive norms can gain power.

For any kind of intervention, we need valid data on actual norms. The important implication of our study is that security-related

norms are also organizational-level phenomena, so collecting data on perceived norms is insufficient. To intervene on valid grounds, one must assess the different types of norms that exist intersubjectively. Thus, organizations should make concerted efforts to identify the unwritten rules among employees and determine how to make them congruent with the formal (written) rules. When the unwritten rules are inconsistent with the desired behavioral change, significant effort must be invested in changing such injunctive norms. Such alignment, recent research shows, should not be based on punishment but on positive incentives and, since communication is the foundation of informal norms, promotion of open communication about security (Rimal and Real, 2003). More specifically, organizations should establish and actively promote communication channels for discussing security. This will not only reinforce shared beliefs but also forge a group identity around security issues. This way, conscious care behavior will become a heuristic way of processing any kind of email.

6.3. Limitations

This study has several limitations that warrant further research. Although collaboration with the KnowBe4 Research gave us access to immensely rich data in terms of the number of employees and organizations, the data were quite limited regarding the number of items and variables in the explanatory mechanism. Most strikingly, this resulted in the inability to control susceptibility to phishing by other variables that have consistently proved important in previous studies. Ideally, we would be able to investigate the empirical support for a model that complements existing psycho-social and information-processing models with our normative framework, taking into account relevant demographic variables (Sheng et al., 2010).

Furthermore, large intra-class correlation coefficients and relatively small explained variances suggest that other relevant organizational factors of susceptibility to phishing exist. Our investigation also did not consider the importance of national culture, which might impact phishing behavior (Flores et al., 2015), the wider organizational security culture, of which norms are a part (DaVeiga and Martins, 2015), or the specific industry to which the organization belongs (Tian et al., 2018). The latter seems to be fruitful terrain for further research, as a recent report (Knowbe4, 2020) indicated that significant differences exist between industries in terms of the percentages of employees that get phished. Our research also indicates that the application of norms theory is complementary with the current models of phishing, and it would be worthwhile to extend the information process and other socio-psychological models by incorporating (organizational-level) normative elements.

Lastly, there are certain methodological limitations that should be addressed in future research. For one, the psychometric quality of the measurement instruments for norms was marginally acceptable, possibly resulting in lower correlations with dependent variables. In designing our items, we wanted to move away from using general or security-specific words—such as “information security” or “phishing”—as the pilot study showed that ordinary employees only vaguely understand them, resulting in socially desirable (yet internally consistent) responses. We, therefore, designed items illustrating abstract concepts, but we obviously sacrificed some internal consistency as a result.

7. Conclusion

To our knowledge, this study is among the first to combine survey data and phishing experiment data to explain the role of individual- and organizational-level security-related norms in susceptibility to phishing in the workplace. It is also one of the few studies to apply a multilevel approach, hailed by organizational researchers as the most suitable approach for researching phenomena that link organizational characteristics with individual behaviors (Costa et al., 2013). One of the central reasons for studying norms emanates from the success of such an approach in other fields, where practical interventions were made that leveraged the persuasive effect of norms to promote socially desirable actions (Jacobson et al., 2020). We believe the finding that norms as sui-generis organizational characteristics impact susceptibility to phishing has important implications for managers and opens a space for developing norm-based interventions that effectively reduce employee susceptibility to email-based phishing and other security-threatening behaviors.

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Gregor Petrič and Kai Roer are founders of CLTRe, a company that was acquired by KnowBe4 in 2019. Kai Roer is employed as Chief Research Officer at KnowBe4.

Acknowledgments

This research was a collaboration between the Center for Informatics and Methodology (Faculty of Social Sciences, University of Ljubljana) and KnowBe4 Research AS, a KnowBe4 research unit. We would especially like to thank Chad Bumpers and Anita Eriksen for technical support in providing the data.

References

Ajzen, I., 1991. The theory of planned behavior. Organ. Behav. Hum. Decis. Process. 50 (2), 179–211.
Aleroud, A., Zhou, L., 2017. Phishing environments, techniques, and countermeasures: a survey. Comput. Secur. 68, 160–196.
Alqahtani, F.H., 2017. Developing an information security policy: a case study approach. Procedia Comput. Sci. 124, 691–697.

Anderson, J.C., Gerbing, D.W., 1991. Predicting the performance of measures in a confirmatory factor analysis with a pretest assessment of their substantive validities. J. Appl. Psychol. 76 (5), 732–740.
Arachchilage, N.A.G., Love, S., 2014. Security awareness of computer users: a phishing threat avoidance perspective. Comput. Hum. Behav. 38, 304–312.
APWG, 2021. Phishing activity trends report. Technical report, Anti-Phishing Working Group, 1st Quarter Report. https://docs.apwg.org/reports/apwg_trends_report_q1_2021.pdf.
Bassett, G., Hylender, C.D., Langlois, P., Pinto, A., Widup, S., 2020. 2020 Verizon Data Breach Report.
Bayl-Smith, P., Taib, R., Yu, K., Wiggins, M., 2021. Response to a phishing attack: persuasion and protection motivation in an organizational context. Inf. Comput. Secur. E-pub ahead of print.
Beenen, G., Ling, K., Wang, X., Chang, K., Frankowski, D., Resnick, P., Kraut, R. E., 2004. Using social psychology to motivate contributions to online communities. In Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work (pp. 212–221).
Bulgurcu, B., Cavusoglu, H., Benbasat, I., 2010. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Q. 34 (3), 523–548.
Burnett, G., Bonnici, L., 2003. Beyond the FAQ: explicit and implicit norms in Usenet newsgroups. Libr. Inf. Sci. Res. 25 (3), 333–351.
Burnett, G., Besant, M., Chatman, E.A., 2001. Small worlds: normative behavior in virtual communities and feminist bookselling. J. Assoc. Inf. Sci. Technol. 52 (7), 536–547.
Byrne, S., Hart, P.S., 2009. The boomerang effect: a synthesis of findings and a preliminary theoretical framework. Ann. Int. Commun. Assoc. 33 (1), 3–37.
Canfield, C.I., Fischhoff, B., Davis, A., 2016. Quantifying phishing susceptibility for detection and behavior decisions. Hum. Factors. 58 (8), 1158–1172.
Canham, M., Posey, C., Strickland, D., Constantino, M. 2021. Phishing for Long Tails: Examining Organizational Repeat Clickers and Protective Stewards. SAGE Open, 11(1).
Chen, R., Gaia, J., Rao, H.R., 2020. An examination of the effect of recent phishing encounters on phishing susceptibility. Decis. Support Syst. 133, 113287. https://doi.org/10.1016/j.dss.2020.113287.
Cialdini, R.B., Bator, R.J., Guadagno, R.E., 1999. Normative influences in organizations, in: Thompson, L.L., Levine, J.M., Messick, D.M. (Eds.), LEA's Organization and Management Series. Shared cognition in Organizations: The Management of Knowledge. Lawrence Erlbaum Associates Publishers, New Jersey, pp. 195–211.
Cialdini, R.B., 2009. Influence: Science and Practice, volume 4. Pearson, Boston, MA.
Conway, D., Taib, R., Harris, M., Yu, K., Berkovsky, S., Chen, F., 2017. A qualitative investigation of bank employee experiences of information security and phishing. In Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017) (pp. 115–129).
Cooke, R.A., Szumal, J.L., 1993. Measuring normative beliefs and shared behavioral expectations in organizations: the reliability and validity of the organizational culture inventory. Psychol. Rep. 72 (3_suppl), 1299–1330.
Costa, P.L., Graça, A.M., Marques-Quinteiro, P., Santos, C.M., Caetano, A., Passos, A.M., 2013. Multilevel research in the field of organizational behavior: An empirical look at 10 years of theory and research. SAGE Open 3(3), 2158244013498244.
Crandall, C.S., Eshleman, A., O'brien, L., 2002. Social norms and the expression and suppression of prejudice: the struggle for internalization. J. Pers. Soc. Psychol. 82 (3), 359.
da Veiga, A., Martins, N., 2015. Improving the information security culture through monitoring and implementation actions illustrated through a case study. Comput. Secur. 49, 162–176.
De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., Ponnet, K., 2018. You've got mail! Explaining individual differences in becoming a phishing target. Telemat. Inform. 35 (5), 1277–1287.
Dequech, D., 2009. Institutions, social norms, and decision-theoretic norms. J. Econ. Behav. Organ. 72 (1), 70–78.
Deutsch, M., Gerard, H.B., 1955. A study of normative and informational social influences upon individual judgment. J. Abnorm. Soc. Psychol. 51 (3), 629–636.
DeVellis, R., 2003. Scale Development: Theory and Applications. Sage Publications, Thousand Oaks, CA.
Downs, J.S., Holbrook, M.B., Cranor, L.F., 2006. Decision strategies and susceptibility to phishing. In: Proceedings of the Second Symposium on Usable Privacy and Security, pp. 79–90.
Durkheim, É., 1982. [first pub. 1895]. The Rules of Sociological Method and Selected Texts on Sociology and its Method. Free Press, New York.
Elster, J., 1989. Social norms and economic theory. J. Econ. Perspect. 3 (4), 99–117.
Fishbein, M., Ajzen, I., 2011. Predicting and Changing Behavior: The Reasoned Action Approach. Psychology Press, New York.
Flores, W. R., Holm, H., Nohlberg, M., & Ekstedt, M., 2015. Investigating personal determinants of phishing and the effect of national culture. Inf. Comput. Secur.23 (2).
Flores, W.R., Ekstedt, M., 2016. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Comput. Secur. 59, 26–44.
Guo, K.H., Yuan, Y., Archer, N.P., Connelly, C.E., 2011. Understanding nonmalicious security violations in the workplace: A composite behavior model. J. Manag. Inf. Syst. 28 (2), 203–236.
Habermas, J., 1985. The Theory of Communicative Action, Volume Two: Lifeworld and System: A Critique of Functionalist Reason. Beacon, Boston, MA.
Hair, J.F., Black, W.C., Babin, B.J., Anderson, R.E., 2014. Multivariate Data Analysis, seventh ed. Pearson, Harlow.
Harrison, B., Vishwanath, A., Ng, Y.J., Rao, R., 2015. Examining the impact of presence on individual phishing victimization. In: 2015 48th Hawaii International Conference on System Sciences, pp. 3483–3489.
Herath, T., Rao, H.R., 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decis. Support. Syst. 47 (2), 154–165.
Hofstede, G., 2001. Culture's consequences, 2nd ed. Sage, Thousand Oaks, CA.
Hosmer Jr, D.W., Lemeshow, S., Sturdivant, R.X., 2013. Applied Logistic Regression, Vol. 398. John Wiley & Sons, Hoboken, New Jersey.
Hox, J.J., Moerbeek, M., Van de Schoot, R., 2017. Multilevel Analysis: Techniques and Applications. Routledge, New York.
Jacobson, R.P., Marchiondo, L.A., Jacobson, K.J.L., Hood, J.N., 2020. The synergistic effect of descriptive and injunctive norm perceptions on counterproductive work behaviors. J. Bus. Ethics 162 (1), 191–209.
Jalali, M.S., Bruckes, M., Westmattelmann, D., Schewe, G., 2020. Why employees (still) click on phishing links: investigation in hospitals. J. Med. Internet Res. 22 (1), e16775.
Kallgren, C.A., Reno, R.R., Cialdini, R.B., 2000. A focus theory of normative conduct: when norms do and do not affect behavior. Pers. Soc. Psychol. Bull. 26 (8), 1002–1012.
Knowbe4, 2020. Phishing by Industry 2020 Benchmarking Report. www.KnowBe4.com. https://info.knowbe4.com/phishing-by-industry-benchmarking-report.
Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M.A., Pham, T., 2009. School of phish: a real-world evaluation of anti-phishing training. In: Proceedings of the 5th Symposium on Usable Privacy and Security, pp. 1–12.
Lebek, B., Uffen, J., Neumann, M., Hohler, B., Breitner, M.H., 2014. Information security awareness and behavior: a theory-based literature review. Manag. Res. Rev. 37 (12), 1049–1092.
Loewenthal, K., Lewis, C., 2015. An introduction to psychological tests and scales. Psychology Press, New York.
Mackie, G., Moneti, F., Shakya, H., Denny, E., 2015. What are Social Norms? How Are They Measured. University of California at San Diego-UNICEF Working Paper, San Diego.
Merhi, M.I., Ahluwalia, P., 2019. Examining the impact of deterrence factors and norms on resistance to information systems security. Comput. Hum. Behav. 92, 37–46.
Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C., Giannakopoulos, G., 2014. The human factor of information security: Unintentional damage perspective. Procedia. Soc. Behav. Sci. 147, 424–428.
Peterson, M.F., Castro, S.L., 2006. Measurement metrics at aggregate levels of analysis: Implications for organization culture research and the GLOBE project. Leadership Q. 17 (5), 506–521.

Piggin, R., 2016. Cyber security trends: What should keep CEOs awake at night. Int. J. Crit. Infrastruct. Prot. 13, 36–38.
Radicati, S., 2020. E-mail Statistics Report, 2020–2024. The Radicati Group Inc., Paolo Alto.
Reno, R.R., Cialdini, R.B., Kallgren, C.A., 1993. The transsituational influence of social norms. J. Pers. Soc. Psychol. 64 (1), 104–112.
Rimal, R.N., Real, K., 2003. Understanding the influence of perceived norms on behaviors. Commun. Theory. 13 (2), 184–203.
Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A., Herawan, T., 2015. Information security conscious care behaviour formation in organizations. Comput. Secur. 53, 65–78.
Schultz, P.W., Nolan, J.M., Cialdini, R.B., Goldstein, N.J., Griskevicius, V., 2007. The constructive, destructive, and reconstructive power of social norms. Psychol. Sci. 18 (5), 429–434.
Schwartz, S.H., 1977. Normative influences on altruism. Adv. Exp. Soc. Psychol. 10 (1), 221–279.
Shahbaznezhad, H., Kolini, F., Rashidirad, M., 2021. Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? J. Comput. Inf. Syst. 61 (6), 539–550.
Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F., Downs, J., 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 373–382.
Smith, J.R., Terry, D.J., 2013. Norms theory. In: Kessler, E.H. (Ed.), Encyclopedia of Management Theory. Sage Publications, Thousand Oaks, CA, pp. 508–511.
Snijders, T.A., Bosker, R.J., 2011. Multilevel analysis: An introduction to basic and advanced multilevel modeling. Sage, London.
Sommestad, T., Hallberg, J., 2013. A review of the theory of planned behaviour in the context of information security policy compliance, in: Janczewski L.J., Wolfe H. B., Shenoi S. (Eds.), Security and Privacy Protection in Information Processing Systems. SEC 2013. IFIP Advances in Information and Communication Technology, vol 405. Springer, Berlin, Heidelberg, pp. 257–271.
Sommestad, T., Karlzén, H., 2019. A meta-analysis of field experiments on phishing susceptibility. In: 2019 APWG Symposium on Electronic Crime Research (eCrime), IEEE, pp. 1–14.
Taib, R., Yu, K., Berkovsky, S., Wiggins, M., Bayl-Smith, P., 2019. Social engineering and organisational dependencies in phishing attacks. In: Lamas, D., Loizides, F., Nacke, L., Petrie, H., Winckler, M., Zaphiris, P. (Eds.), IFIP Conference on Human-Computer Interaction. Springer, Cham., pp. 564–584
Taylor, F.W., 1911. The Principles of Scientific Management. Harper & Brothers, New York, NY and London, UK.
Tian, C., Jensen, M.L., Durcikova, A., 2018. Phishing susceptibility across industries: the differential impact of influence techniques. In: Proceedings of the 13th Pre-ICIS Workshop on Information Security and Privacy, pp. 1–20.
Vance, A., Siponen, M., Pahnila, S., 2012. Motivating IS security compliance: Insights from habit and protection motivation theory. Inf. Manag. 49 (3-4), 190–198.
Vishwanath, A., Herath, T., Chen, R., Wang, J., Rao, H.R., 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.
Vishwanath, A., Harrison, B., Ng, Y.J., 2018. Suspicion, cognition, and automaticity model of phishing susceptibility. Commun. Res. 45 (8), 1146–1166.
Wang, J., Herath, T., Chen, R., Vishwanath, A., Rao, H.R., 2012. Phishing susceptibility: an investigation into the processing of a targeted spear phishing email. IEEE Trans. Prof. Commun. 55 (4), 345–362.
Wiafe, I., Koranteng, F.N., Wiafe, A., Obeng, E.N., Yaokumah, W., 2020. The role of norms in information security policy compliance. Inf. Comput. Secur. 28(5), 743–761.
Williams, E.J., Hinds, J., Joinson, A.N., 2018. Exploring susceptibility to phishing in the workplace. Int. J. Hum. Comput. Stud. 120, 1–13.
Yazdanmehr, A., Wang, J., 2016. Employees' information security policy compliance: a norm activation perspective. Decis. Support Syst. 92, 36–46.