The Influence of Human Factors on the Intention to Report Phishing Emails

Ioana Marin
Eindhoven University of Technology
Netherlands
i.a.mar@hotmail.com

Pavlo Burda*
Eindhoven University of Technology
Netherlands
p.burda@tue.nl

Luca Allodi
Eindhoven University of Technology
Netherlands
l.allodi@tue.nl

Nicola Zannone
Eindhoven University of Technology
Netherlands
n.zannone@tue.nl

ABSTRACT

Phishing attacks are a main threat to organizations and individuals. Current widespread defenses based on spam filters and domain blacklisting are unfortunately insufficient. Prior work identifies phishing reporting as a key, largely untapped resource to mitigate phishing threats. Yet, its practice suffers from very low reporting rates and generally too low an uptake from users. Whereas it is known that phishing reporting behavior is affected by a number of 'human factors', a comprehensive view of the different theories and their effects on (intent to) report is not yet developed. To address this gap, we evaluate theories and factors analyzed in the extant literature, build a cohesive theoretical view of their effects and constructs, and develop, model, and empirically evaluate (by means of an online questionnaire, n=284) the resulting hypothesis structure. We discuss both theoretical implications of our findings and research directions for practice at a research and organizational level.

CCS CONCEPTS

• **Security and privacy → Social engineering attacks**; • **Human-centered computing → Empirical studies in HCI**; • **Social and professional topics → Phishing**.

KEYWORDS

Information Security; Cyber security behaviors; Organizational citizenship behaviors; Personality traits.

ACM Reference Format:
Ioana Marin, Pavlo Burda, Luca Allodi, and Nicola Zannone. 2023. The Influence of Human Factors on the Intention to Report Phishing Emails. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 18 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

*Main contact author

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Phishing is one of the most prominent attack vectors employed in modern cyber attacks. In a phishing attack, the attacker sends a deceptive message to a user (of a platform, or an employee of an organization) with the goal of tricking them into revealing sensitive data (e.g., passwords or credit card information) or executing malicious code (e.g., by opening an attachment or visiting a website) granting remote access to the platform or system to the attacker. According to recent reports, phishing plays a role in approximately 43% of registered data breaches [60], and in the US alone, in 2020, led to a loss of over 54M USD [12]. Part of the reason why phishing attacks remain so successful is that current phishing countermeasures mainly focus on detection techniques based on spam filters and blacklisting of phishing domains, which have proven insufficient particularly to detect more targeted variants of these attacks [2]: spam filters are oftentimes incapable of detecting well-engineered, credible phishing attacks, and the speed by which these achieve their objectives makes blacklisting simply too slow to be effective in time (i.e., before the attack targets have been victimized) [8].

Recent work has stressed the importance of phishing reporting as an additional [3], potentially fast [8], crowd-source based countermeasure to timely react and mitigate phishing attacks. Phishing reporting is a practice adopted in most organizations (either by internal means or by reporting tools provided by major software platforms, such as Microsoft's Office365) that counts on the organization's employees to report suspicious messages, generally in the form of emails [3], to the organization. Reporting is increasingly more prevalent in phishing awareness material and training exercises, yet phishing reporting rates remain steadily below 10% [30, 61].

How to maximize and fully exploit the additional line of defense represented by phishing reporting remains an open question. Human factors such as personality traits [11], employees' attitudes towards the organization [41] and towards their own colleagues have been shown to play an effect on individuals' cyber security behaviors, in general, [23], but the overall picture remains fragmented, and therefore not yet actionable, in the literature [30]. We argue that a full picture can only be derived by looking at both an individual (e.g., personality traits) and organization (e.g., relating to employees' security assurance behaviors and compliance to security policies) perspective simultaneously and by focusing on phishing reporting behaviors (as opposed to generic cyber security

behaviors). Moreover, the lack of a single theoretical picture linking together different relevant theories in a cohesive framework limits the reusability and actionability of findings. Importantly, 'extra-role' behaviors (e.g., those not necessarily mandated or motivated by an organization's policy) have not yet been considered in the picture.

To address these gaps, in this study we unify different perspectives pertaining to human traits and organizational cyber security behavior towards both the organization itself and individuals, and evaluate their joint effect on the intention to report phishing emails. We formulate the following research question:

RQ: *How do human factors, pertaining to the individual and the organizational levels, influence the intention of reporting suspicious phishing attacks?*

To answer our research question, we first evaluate the extant literature to identify theories and factors pertaining to individual and organization-level cyber security behaviors, and personal characteristics such as beliefs and the 'Big Five' personality traits. Based on these, we derive our hypotheses and construct a unified theoretical model of the human factors affecting an individual's intention to report phishing emails. The model and hypotheses structure are used to create an online questionnaire aimed at empirically evaluating and quantifying the link between the identified factors, their relation, and their joint effect on individuals' cyber security behavior and their intention to report phishing emails. We conduct the survey on Amazon Mechanical Turk (AMT) with 284 participants. The main contributions of this paper are as follows:

- The developed hypothesis structure and related theoretical model address the fragmentation of the extant literature by providing a cohesive picture of individual and organizational factors, affecting individuals' cyber security behaviors and their intention to report phishing emails, and their interplay.
- Our empirical evaluation shows that accounting for different types of human factors (personality traits, beliefs, attitudes towards the organization and co-workers) at both individual and organization levels provides a more comprehensive understanding of their effects on individuals' positive cyber security behaviors and intention to report phishing emails. For example, emotional stability and extraversion traits are not aligned with previous results on cyber security behaviors, potentially due to the inclusion of other factors such as organization-related factors.
- Our evaluation also shows that the human factors that influence an individuals' cyber security behaviors, in general, might differ from the factors influencing a specific cyber security behavior such as the reporting of phishing emails. For instance, conscientiousness and extraversion appear to have a strong relationship with generic cyber security behaviors, but this does not translate to the specific behavior of reporting; to the contrary, we observed that altruism only influences reporting.
- The understanding of the effects of human factors has implications at both a theoretical and practical level and can help organizations to improve their overall security posture. Our findings can support researchers and practitioners in the design of better training practices and awareness programs and can help organizations to create a security culture. For instance, our results show that high-sportsmanship individuals, who usually tend to avoid filing complaints, are characterized by a lower intention to report phishing emails; a training program may mitigate this effect by stressing the relevance of phishing reporting in terms of increased overall security.

The remainder of the paper is structured as follows. The next section introduces the relevant theoretical background on information security behaviors and their relation with human factors. Section 3 presents our hypotheses and Sections 4 presents the methodology to test those hypotheses. Section 5 presents the results and Section 6 discusses the implications and relevance of our findings at both a theoretical and practical level, as well as the limitations of our study. Finally, Section 7 concludes the paper.

2 BACKGROUND AND RELATED WORK

To protect their sensitive information and assets, organizations not only employ various types of security mechanisms but also take measures to improve their security posture. To this end, organizations often engage their employees with security *training* programs to educate them, for instance, on how to detect and report phishing scams, and with phishing *awareness* programs to ensure that they become familiar with how phishing attacks are deployed, recognize when they are the target of a suspicious phishing email and react accordingly [46]. More in general, organizations often aim to create a security *culture* providing their employees a pattern of shared basic assumptions and principles that work well enough to be considered valid and, therefore, shape employees' perception and behaviors adopted within the organization [52]. Therefore, organization culture, training and awareness are clearly involved in shaping employees' positive cyber security behaviors and may be valuable tools to mold phishing reporting behaviors. However, their effectiveness and uptake often depends on the employees' experiences, personality traits, characteristics and beliefs.

The cognitive science field, applied to the InfoSec domain, provides the foundation of the current study as it identifies the human factors involved in the cognitive processes that emerge when encountering a phishing email. A number of theories have been proposed to understand the relationship between human factors and the intention of an individual to engage in performing an action [1, 50]. In this work, we apply these theories to positive cyber security behaviors with a particular focus on users' intention to report phishing emails. Next, we provide an overview of the most influential concepts that aim to explain InfoSec-related behaviors, that will form the basis of our research model.

2.1 Reasoning on InfoSec-related Behaviors

Cyber Security Behavior Classification. Guo [16] proposes a framework to classify employees' InfoSec-related behaviors observed in organizations. These behaviors are structured into four categories: *Security Assurance Behavior (SAB)*, *Security Compliant Behavior (SCB)*, *Security Risk-taking Behavior (SRB)*, and *Security Damaging Behavior (SDB)*. The first two categories, SAB and SCB, focus on the desired behaviors that an organization should encourage, while the latter two categories, SRB and SDB, are the behaviors that an organization should prevent. Specifically, SAB describes behaviors that an employee actively performs with the intention to protect the organization's systems (e.g., reporting security incidents), whereas SCB describes both intentional and unintentional behaviors aimed

Table 1: OCB Characteristics

Class	Characteristic	Description
OCBO	Civic Virtue	This trait represents an individual's non-obligatory concerns regarding the welfare of the organization as a collective, creating a sense of community by including their voluntary active participation towards solving existing issues and improving the organization's processes.
	Leader Support	This characteristic covers the employee's perception of positive behaviors received from their superiors. Such behaviors include both task-oriented actions (e.g., receiving help with ongoing projects, appropriately setting goals and deadlines), and socio-emotional actions (e.g., effective communication and interaction) [4].
	Organizational Commitment	This characteristic refers to the *Affective* Organizational Commitment, which captures an individual's connection with the organization's values and objectives, while displaying similar views that lead to beneficial behaviors.
	Sportsmanship	This characteristic covers an individual's tolerance for less-than-ideal situations encountered within the organization, when, even though they might not fully agree with or be aware of the circumstances, employees do not display complaining or negative behaviors.
	Conscientiousness	This characteristic represents a narrower form of generalized compliance [33], involves self-discipline, and refers to employees whose helping behaviors exceed simply adhering to the rules and obligations prior established by the organization.
	Job Satisfaction	This characteristic indicates the employee's contentedness with their workplace, including their perception of different aspects related to the type of job they perform, or the organization they are associated with.
OCBI	Altruism	This characteristic defines the extra-role behaviors that are directly intended to assist or provide support to others in an organizational setting (e.g., helping co-workers by taking some of their tasks, or volunteering to perform an action that is not required) [33].
	Courtesy	This characteristic refers to performing considerate actions with the goal of avoiding problems that could occur or impact the organization (e.g., "Is mindful of how his or her behavior affects other people's jobs") [28].

to comply with an organization's Information Security Policy (ISP). On the other hand, SRB describes intentional behaviors that could harm an organization's data security (e.g., writing sensitive data on paper), while SDB describes intentional behaviors of an employee that directly damage the organization (e.g., data theft). As here we focus on phishing reporting, in this work we only consider positive behaviors, namely SAB and SCB, to which we refer as *Positive Cyber Security Behaviors*.

Organizational Citizenship Behaviors (OCB). OCB refers to "individual behavior that is discretionary, not directly or explicitly recognized by the formal reward system, and that in the aggregate promotes the effective functioning of the organization" [40, p. 86]. Since its introduction, OCB has attracted much attention from the research community to identify and analyze the relationship between various behavioral dimensions, known as predictors, that impact OCB. Following the division proposed in [65], OCB is refined into two distinct subgroups of characteristics, depending on the target of the behavior: OCB directed towards the Organization (OCBO) and OCB directed towards Individuals (OCBI). In the InfoSec context, OCBs influence both positive and negative cyber security behaviors [11]. In particular, OCB is linked to behaviors supporting and reducing potential InfoSec harm in an organization (SAB and SCB).

2.2 Human Factors

Next we discuss, from the extant literature, the most relevant human factors affecting the intentions and actions of individuals from a cyber security perspective.

OCB Characteristics. Several studies have investigated OCB characteristics and their implications on behaviors related to InfoSec. An overview of these characteristics is presented in Table 1. Helping/supporting behaviors towards the organization and co-workers are generally beneficial to the organization's cybersecurity posture. Within OCB characteristics directed towards an organization (OCBO), *Sportsmanship* is known to have a notable impact on the overall predisposition of individuals to be helpful in organizational contexts [33], where individuals with a high level of Sportsmanship are less prone to have negative reactions and complain about current issues as they are more oriented towards future improvements and their contribution to these changes [51]. Employees' purposeful help and support directed at the organization when solving encountered issues is influenced by their level of *Civic Virtue*, which influences the direct contribution of employees in the protection of the organization they work for [49]. Differently, the motivation behind employees' beneficial behaviors is driven by *Organizational Commitment*, which is typical of employees that share the organization's views and ideals (*cf.* culture, above) [46].

At the *individual* level of OCB, *Altruism* and *Courtesy* are OCBI characteristics that relate to actions directly intended to help co-workers [22, 56] and contribute to the smooth functioning of the organization [56]. In particular, it has been shown that Altruism improves employees' overall performance in executing their daily tasks and the collective efficiency of the organization [22]. Differently, employees showing a high level of Courtesy are inclined to perform actions that help avoid or mitigate potential issues, cautiously engaging in any behaviors that may harm their co-workers [51].

Security assurance and compliance behaviors include actions that individuals perform with the aim of protecting the organization from potential security attacks. These behaviors are often associated with a high level of Conscientiousness: conscientious individuals tend to go beyond the minimum requirements and actively engage in security behaviors [18, 22, 51]. This characteristic influences an individual's work ethic and behavior consistency; related to email usage, a high level of Conscientiousness leads to the inclination to regularly check emails and thoroughly evaluate the information of the received emails, resulting in a lower susceptibility to phishing attacks [30]. However, when this repeated behavior is exhibited by individuals with low emotional stability, it may lead to strong email habits [63] such as constantly monitoring email and regularly engaging with links in emails they receive.

Table 2: The Big Five dimensions of personality

Dimension	Description
Agreeableness	This dimension includes interpersonal characteristics related to being courteous, flexible, trusting, cooperative, tolerant, and forgiving [7].
Conscientiousness	This dimension involves dependability, namely being careful, thorough, responsible, organized, and planful [7].
Openness to Experience	This dimension reflects an individual's imaginative, cultured, curious, original, broad-minded, intelligent, and artistically sensitive aspects [7].
Extraversion	This dimension includes interpersonal characteristics related to sociability, gregariousness, assertiveness, talkativeness, and activeness [7].
Emotional Stability	This dimension covers an individual's emotional adjustments, observing the lack of anxiety, anger, embarrassment, worry, insecurity, and impulsiveness [7].

The Big Five Theory Characteristics. The Big Five Theory aims to measure and interpret individuals' personality variations, guided by five defined factors characterizing independent human cognition dimensions [36, 39]. The five dimensions of personality traits are: *Agreeableness/Likability*, *Conscientiousness*, *Openness to Experience*, *Extraversion/Surgency*, and *Emotional Stability* (inverse of Neuroticism or Cognitive Impulsivity). An overview of these dimensions is provided in Table 2.

Considerable research has been conducted to study the relationship between the "Big Five" personality traits and how these affect the underlying cognitive processes involved in the InfoSec context, including the actions an individual takes when receiving a phishing email [26, 37, 63]. In particular, it has been shown that these dimensions are strong predictors of proactive behaviors related to security assurance behaviors within organizations [11]. For instance, previous research investigated the influence of high cognitive impulsivity on email management, finding supportive evidence that individuals with low *Emotional Stability* tend to be more volatile and, therefore, more likely to engage in behaviors that damage the organization [11], while less impulsive employees are better at evaluating and managing phishing emails [43]. Similarly, individuals characterized by a high level of *Extraversion* are typically able to handle phishing emails and take appropriate actions, including reporting the suspicious email received, even if they are not completely certain it is phishing [43]. Individuals with higher levels of *Agreeableness* and *Openness to Experience* tend to be more receptive of the organization's security training [11]. *Conscientious* individuals are also aware of their organization's rules and regulations and may aspire to adhere to them [11]. Therefore, they usually comply with information security policies and guidelines established by their organization. On the other hand, individuals with low levels of Conscientiousness and Agreeableness may not consider the implications of their behaviors or even deliberately act against their organization if it benefits them [11].

Beliefs. Beliefs refer to subjective interpretations, focusing on one's attitude or perception about a 'truth' that has not been verified, and are known to influence human behaviors. In the context of Social Engineering (SE) attacks within organizational settings, the leading beliefs that affect an individual's behavioral attitude are *Self-efficacy*, *Subjective Norms* and *Habits*, briefly described in Table 3.

Self-efficacy and Subjective Norms are beliefs that can influence employees' compliance behaviors within the organization they are part of. Self-efficacy is a dimension of coping appraisals within the Protection Motivation Theory (PMT) [50] and represents "the most powerful predictor of intention to comply with a behavior" [55, p. 218]. This type of belief influences both employees' competence and effort put into the work-related activities, as well as how behavioral patterns evolve [1]. At an organizational level, more experienced and confident individuals are shown to be less inclined to comply with the demands of a deceptive email [66]. In contrast, it was observed that individuals who self-rated their technical knowledge as low are more likely to be subject to phishing [18, 54]. On the same line, the Theory of Planned Behavior (TPB) [1] shows that Subjective Norms, together with an individual's attitude towards a behavior and perceived controls, can be used to predict an individual's intention to perform that behavior with a high accuracy degree in organizational contexts. The relevance of Subjective Norms with respect to an employee's cyber security behaviors has also been studied by Jalali et al. [23], who observed that Subjective Norms positively affect an individual's intention to comply with the ISP of the organization.

Self-efficacy, together with Habits, is also an influential factor for security assurance behaviors. Kwak et al. [30] studied the role of Self-efficacy as a predictor of the likelihood of *reporting* spear phishing emails, showing that individuals with higher levels of Self-efficacy put great effort into reporting, whereas individuals with lower levels of Self-efficacy have self-doubt and do not take further actions. On the other hand, recent research shows that *Email Habits*, i.e. non-intentional automatic behaviors related to email usage, is a predictor of the intention to click on phishing emails [53].

2.3 Discussion on related work

Several works in the multidisciplinary domains of InfoSec and cognitive sciences investigate the human factors impacting behaviors aimed at protecting sensitive information or relating to deception. However, previous studies have mainly focused on general positive and negative cyber security behaviors in organizational contexts, covering human factors involved in the beneficial and harmful behaviors individuals perform [11], but little attention has been given to human factors impacting intention to report. Recent work on reporting has investigated, for instance, whether using the employees as a collective phishing detection mechanism is practical in large organizations [8, 31], the relationship between the believability of a phishing email and the associated reporting rate [25] or how security gamification can improve phishing reporting [24]. A few studies have focused on individuals' behaviors towards phishing emails, for instance, by investigated the reasoning behind why individuals open suspicious emails [23, 53] or the motivations of why phishing reporting is scarce [30]. However, an understanding of which human factors influence an individual's propensity to report suspicious email is still lacking. Moreover, the vast number of different theories and classifications may hinder the development of a clear overview of the impact that human factors have on phishing

Table 3: Dimensions of Beliefs

Dimension	Description
Habits	Following the Habit Theory, this type of belief refers to "...learned acts that become automatic responses to situations, which can be functional in obtaining certain goals or end-states" [62, p. 112]. Behaviors performed with repetition under certain cues have the tendency of becoming habitual, where fewer conscious decisions are required.
Subjective Norms	This characteristic concerns the beliefs an individual has regarding a perceived social pressure, namely whether others would approve or disapprove of them performing a behavior. From an organizational perspective, subjective norms are cues that individuals within an organization urge employees to take in order to perform certain actions [1].
Self-efficacy	Self-efficacy represents an individual's confidence that they are capable of performing response behaviors to encountered data security incidents [64]. This behavior can be achieved by adhering to the established ISPs (as a part of SCB), as well as consciously performing actions that lead to the active protection of organizational data (as a part of SAB). More specifically, self-efficacy points to an individual's belief that they can perform anti-phishing behaviors, such as reporting an email received that they have identified as being suspicious.

reporting. Previous research has mainly focused on the factors that influence in-role behaviors of employees by adhering to ISP [55], while the extra-role behaviors influencing an individual's cyber security actions at their workplace have not yet been assessed.

In this work, we investigate the human factors that influence individuals' cyber security behaviors in organizational contexts and their intention to report phishing emails. To this end, we employ the human factors identified in previous studies, especially concerning actions related to phishing emails, as a baseline for the current research (cf. Section 3). Thus, this work adds to the current literature by focusing on the human factors that influence behaviors related to phishing reporting, at *both* organization and individual level.

3 HYPOTHESIS DEVELOPMENT

In Section 2 we identified the human factors and theories that the extant literature has related to cyber security behaviors. We employ those perspectives to derive a theoretical model of human factors, setting the hypotheses tested in this work. To keep the size of the experiment manageable, for each variable category (OCBO, OCBI, personality traits, and beliefs) we select two variables for which the literature reports evidence of their relevance for the security constructs in our model. A more extensive justification of the inclusion of each variable is given in Sections 3.1 to 3.3.

Figure 1 provides a graphical representation of the selected constructs and related hypotheses. The model comprises eight constructs representing the human factors that can potentially influence an individual's cyber security behaviors and their intention towards the reporting of phishing emails. The hypotheses are divided in three groups: the first group investigates which human factors positively affect positive cyber security behaviors; the second group investigates whether positive cyber security behaviors positively influence an individual's intention to report phishing emails; and the third group investigates which human factors positively relate to the intention to report phishing emails.

3.1 Human Factors affecting Positive Cyber Security Behaviors

Previous work has shown that OCB characteristics and personality traits influence an individual's cyber security behaviors [26, 37], but they were typically studied separately. In this work, we are interested in assessing their combined effects on an individual's positive cyber security behaviors. Among the OCBO characteristics, it has been observed that *Conscientiousness* and *Sportsmanship* are strong predictors of organizational and security behaviors, where individuals with a high level of Sportsmanship are significantly more likely to engage in behaviors that contribute to the good welfare of the organization [51], and Conscientiousness is positively associated with secure behaviours [18] and positively affects how targets respond to received phishing emails [30]. As seen in Section 2.2, *Altruism* and *Courtesy* display a strong positive correlation with OCB and are prominent predictors for relevant human behaviors associated with helping coworkers, mitigating and avoiding issues [22, 51, 56] which reasonably fall within the scope of positive cyber security behaviors. In terms of email usage, we aim to test whether individuals who tend to be less impulsive in their decision-making processes and more extraverted, are also more likely to perform proactive security actions as these personality traits are more relevant for an individual's cyber security behaviors compared to other traits. Indeed, as shown in previous studies, individuals with low cognitive impulsivity are more likely to take measures against phishing attacks [9]; similarly, extraverted individuals typically take the appropriate action to handle both genuine and phishing emails [37]. Therefore, we consider *Emotional Stability* and *Extraversion* in our research model. As a result, the following hypotheses are used to test the relationship between the identified factors and positive cyber security behaviors:

H1.1: *Sportsmanship is positively related to an individual's Positive Cyber Security Behaviors.*

H1.2: *Conscientiousness is positively related to an individual's Positive Cyber Security Behaviors.*

H1.3: *Altruism is positively related to an individual's Positive Cyber Security Behaviors.*

H1.4: *Courtesy is positively related to an individual's Positive Cyber Security Behaviors.*

H1.5: *Emotional Stability is positively related to an individual's Positive Cyber Security Behaviors.*

H1.6: *Extraversion is positively related to an individual's Positive Cyber Security Behaviors.*

3.2 Positive Cyber Security Behaviors affecting the Intention to Report Phishing Emails

A large body of research has studied individuals' cyber security behaviors within an organization setting, also in the context of phishing attacks. Previous work has often investigated either abstract cyber security behavior constructs, such as PCSBs, or specific cyber security behaviors, such as managing emails or clicking on links. However, in the former case the resulting findings and considerations were often extended and generalised to specific cyber security

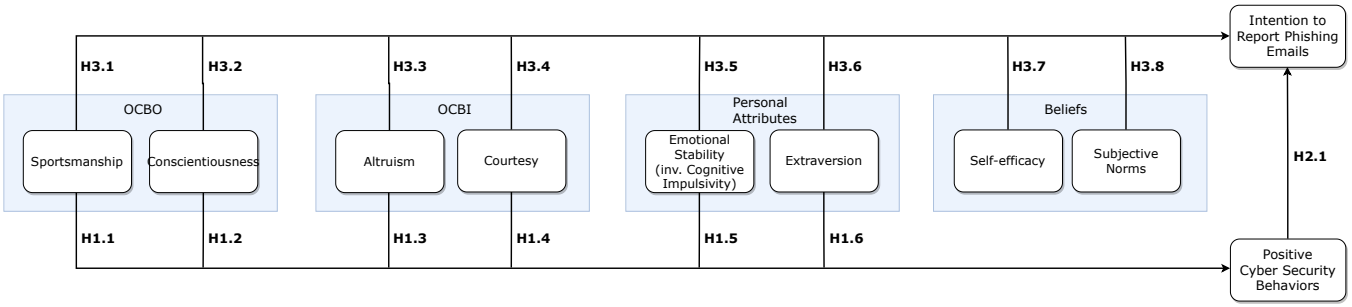

Figure 1: Research model

behaviors, and vice versa for the latter case. Such generalizations and extensions of findings from generic to specific behaviors (or from specific to generic) might not always hold. Moreover, previous studies typically focus on phishing victimization (opening a phishing email or clicking on the link) while an understanding of the actions an individual may perform to *protect* the organization from phishing attacks is far less studied. To fill these gaps, we investigate whether positive cyber security behaviors influence an individual's intention to report phishing emails, when both extra-role (SAB) and in-role (SCB) behaviors are considered:

H2.1: *Positive Cyber Security Behaviors are positively related to an individual's intention to report emails that they consider to be phishing.*

3.3 Human Factors affecting the Intention to Report Phishing Emails

Although several works have studied whether human factors influence an individual's cyber security behaviors (cf. Section 2.2), it is still unclear whether they also affect the intention to report phishing emails, especially when reporting requires additional efforts. To this end, in addition to the OCB characteristics and personality traits discussed in Section 3.1, we also study how beliefs influence the intention to report suspicious emails. In particular, we study the relation between beliefs and an employee's compliance intentions (in-role behaviors) and analyze whether this knowledge can be extended to the employee's active commitment to protect the organization outside of the described policies and regulations (extra-role behaviors). Among the types of beliefs discussed in Section 2.2, we consider *Subjective Norms* and *Self-efficacy* as these human attitude and perception factors can alter an individual's behavioral intentions in the context of reporting suspicious emails. On the other hand, we do not consider *Habits* as they represent behaviors performed with repetition, where fewer conscious decisions are required [63]. The observations above are captured by the following hypotheses:

H3.1: *Sportsmanship is positively related to an individual's intention to report emails that they consider to be phishing.*

H3.2: *Conscientiousness is positively related to an individual's intention to report emails that they consider to be phishing.*

H3.3: *Altruism is positively related to an individual's intention to report emails that they consider to be phishing.*

H3.4: *Courtesy is positively related to an individual's intention to report emails that they consider to be phishing.*

H3.5: *Emotional Stability is positively related to an individual's intention to report emails that they consider to be phishing.*

H3.6: *Extraversion is positively related to an individual's intention to report emails that they consider to be phishing.*

H3.7: *Self-efficacy is positively related to an individual's intention to report emails that they consider to be phishing.*

H3.8: *Subjective Norms are positively related to an individual's intention to report emails that they consider to be phishing.*

4 METHODOLOGY

To analyze to which extent human factors affect an individual's intention to report phishing emails and, thus, to test the hypotheses presented in Section 3, we conducted an online survey on Amazon Mechanical Turk (AMT) [5], with a sample size of $n = 284$ participants.[1] The respondents were required to answer a questionnaire to assess their characteristics as well as their cyber security behavior and willingness to report phishing emails. A number of checks were employed to assess the reliability of the data [57]; only responses that passed these checks were considered for hypothesis testing.

4.1 Subject Selection

We recruited the participants of our study on AMT. To ensure the quality of the collected data, we required respondents to have a minimum of 1000 previously approved tasks on the platform with an acceptance rate of at least 98%. We also recruited participants only from the US. This choice was made to maintain a high likelihood of having fluent English speakers and to avoid fragmentation in the respondent population. We discuss implications to generalizability of our results in Section 6.3.

We follow recent practice underlying the importance of detecting and discarding incorrect responses to maintain a high reliability for studies run on AMT [25, 57]. Following [25], we employ four checks to ensure that unreliable respondents are excluded from data analysis. The four checks are as follows. At the beginning of the survey, participants were required to provide their AMT WorkerID. We removed surveys for which the WorkerID provided by

[1]We determine the minimum sample size to obtain a statistical power of 90% by conducting a pilot study involving 100 participants and calculate the final sample size following [34] (full calculations in Appendix B). This estimation yielded a required sample size of $n = 267$. Accounting for an estimated 10% of faulty responses, the estimated total sample size for conducting the survey was rounded up to 300 participants. Accordingly, we recruited 200 additional participants for our study.

Table 4: Regression Equations corresponding to the three models

Model	Dependent Variable	Equation
1	Positive Cyber Security Behaviors ($PCSB$)	$PCSB_i = \beta_0 + \beta_1 \cdot Sportsmanship_i + \beta_2 \cdot Conscientiousness_i + \beta_3 \cdot Altruism_i + \beta_4 \cdot Courtesy_i + \beta_5 \cdot EmotionalStability_i + \beta_6 \cdot Extraversion_i$
2	Intention to Report Phishing ($RepInt$)	$RepInt_i = \beta_0 + \beta_1 \cdot PositiveCyberSecurityBehaviors_i$
3	Intention to Report Phishing ($RepInt$)	$RepInt_i = \beta_0 + \beta_1 \cdot Sportsmanship_i + \beta_2 \cdot Conscientiousness_i + \beta_3 \cdot Altruism_i + \beta_4 \cdot Courtesy_i + \beta_5 \cdot EmotionalStability_i + \beta_6 \cdot Extraversion_i + \beta_7 \cdot SubjectiveNorms_i + \beta_8 \cdot SelfEfficacy_i$

Notes: To aid comparison, we report standardized β coefficients. Hence β_0 is centered at 0 for all models. Error terms not reported for brevity.

the participant did not match any WorkerID in the list of participants we gathered from the AMT platform for this task, or the same WorkerID occurred multiple times to prevent double entries from a single subject. We also included an attention check question in the survey and only considered the responses of those participants who answered that question correctly. In addition, at the end of the survey, participants had to provide a survey completion code to demonstrate that they have completed the survey. Finally, all participants who completed the survey within 5 minutes[2] were rejected and removed from the experiment. Based on these checks, we discarded 16 participants (5% of respondents); answers from the remaining 284 subjects were included in the analysis.

4.2 Survey Design

Our survey aims to assess the human factors influencing an individual's positive cyber security behaviors and intention to report phishing emails. The survey consists of four parts. After a short introduction about the notion of reporting and the purpose of the survey, the participants were asked to provide their demographics, such as their age, education, and current occupation (cf. Table 13 in Appendix C). The second part of the questionnaire comprises questions focusing on the respondents' personality traits and other factors related to their routines at the workplace (i.e., OCB characteristics). The last two sets of questions aim to measure a participant's beliefs, positive cyber security behavior, and intention to report phishing emails, respectively. The survey also includes an open question that allows the participants to share their views regarding why anyone would or not be willing to report suspicious emails. An overview of the survey questions is provided in Appendix C (Table 14).

To reduce ambiguity and biases in the interpretation of the questions, we took several steps. First, we based the survey items, used to measure the human factors, on existing assessment methods [11, 15, 44, 53] and adapted them to minimize ambiguity and maximize the fit in the context of phishing email reporting. Then, we ran three review rounds. In the first review round, we consulted relevant literature [10, 47] to minimize common pitfalls in questionnaire wording. In the second review round, we administered the questionnaire to six PhD students who provided feedback regarding the clarity of the survey items. Finally, the survey was reviewed by a native English speaker with the specific aim of identifying any remaining ambiguous wording. The gathered feedback was discussed among the authors, and the wording of the questions was finalized accordingly until no further ambiguities or points of improvement emerged.

We used a five-point Likert scale with six items to measure positive cyber security behaviors and four items to measure all the other constructs. Similarly, the attention check question item asks the participants to select a particular choice from the same five-point scale. To minimize ambiguity in the responses, we relied on [47, 59] to choose our wording to define the scale over which users rate their responses. When performing the analysis of the results, the measured factors of each participant are calculated as the average of the answers provided across all items for that specific variable.

[2]The expected completion time of the survey is 20 minutes.

4.3 Data Analysis

Respondent Demographics. From the answers gathered from the demographic questions in the survey, we first analyzed, by means of their (Pearson) correlation, the relationship of the respondent's demographics with their *positive cyber security behaviors* and *intention to report phishing emails*. This analysis was used to provide descriptive statistics of the survey participants and to provide context for collected respondent data regarding their intention to report suspicious emails.

Reliability and Validity of the Measured Variables. Before assessing the hypotheses, we determined the reliability and validity of the measured items. Following [27] we measure the internal consistency of the measured variables by calculating the Cronbach's α value of the corresponding items, and set the threshold for a satisfactory outcome to 0.7. We also assessed the discriminant validity of the model variables by computing the correlation across the independent and dependent variables to check for multicollinearity problems. Following [17], we assume that there is no multicollinearity if the correlations across all pairs of variables are below the recommended threshold value of 0.8.

Hypothesis Evaluation. To evaluate the hypotheses presented in Figure 1, we devised three regression models, one for each group of hypotheses. Model 1 encompasses the hypotheses presented in Section 3.1 and aims to assess the effect of the OCB characteristics and personality traits on positive cyber security behaviors. Model 2 addresses the hypothesis of Section 3.2 and aims to assess the influence of positive cyber security behaviors on an individual's intention to report phishing emails. Finally, Model 3 formalizes the hypotheses of Section 3.3 and aims to measure the effect of all identified human factors on the intention to report phishing emails. An overview of the regression equations corresponding to the three models is given in Table 4.

We performed a linear regression using the Ordinary Least Squares (OLS) Estimation [20]. When presenting the results of the regression analysis in Section 5.3, we report the standardized coefficients of the independent variables to compare the relative magnitude and sign of the effects of these independent variables on the dependent variable.

We perform and report the regression analysis on the three models with and without control variables, where the control variable are derived from the demographic information elicited through the survey (cf. Section 4.2). This was to determine the extent to which the control variables modulate the effect of the observed independent variables, which may be an index of additional hidden effects in the models. The results of the regression analysis were used for the evaluation of the hypotheses. We consider factors whose regression coefficients have a p-value lower than 0.05 as statistically *significant*. We note that our hypotheses are directional, hence we only reject the respective null hypotheses when both coefficient sign and statistical significance are aligned with the (statistical validity of the) prediction.

4.4 Ethical Aspects

This research was executed under ethical approval from our institution's ethical review board under approval number `ERB2020MCS13`. Participants' WorkerIDs were not transmitted in any form to minimize any risks to our survey's participants. The participants were assured that their answers are used for research purposes only. In the design of the questionnaire, we followed ethical practices for response options [47]. Additionally, in line with the US federal minimum wage of $7.25 per hour [58], each participant that delivered a valid survey response received a compensation of $2.7. With an average completion time of 21 minutes, this equates to an hourly compensation of $7.7.

5 RESULTS

After conducting the pilot and the main survey, the total dataset consisted of 284 valid responses. In this section, we first present the descriptive statistics of the respondents and control correlations. Then, we report on the results of the factor reliability and the linear regressions used for testing the hypotheses presented in Section 3.

5.1 Respondent Demographics

Table 5 presents an overview of the demographic information of the 284 participants to our survey. For each control variable, the table reports the frequency and percentage of the participants' answers. We can observe that a similar proportion of male and female participants were part of the survey. Moreover, our sample comprises approximately 60% of adults between 31-50 years of age and most have at least a college education. In line with this profile, 50% of the respondents report being in senior (i.e., not entry-level) job positions. A perhaps surprising statistic emerging from the sample is the seemingly high (45%) fraction of respondents that indicate having fallen for a phishing email. A possible explanation is that the type of task focused on phishing in organizations attracted users with previous experience on the topic. We comment on possible implications for external validity in Section 6.3.

Table 6 reports an overview of the linear relations between the control variables and an individual's *positive cyber security behaviors* (top rows) and *intention to report phishing emails* (bottom rows). Three of the eight selected controls, namely *Education*, *Current employment duration*, and *Reporting frequency*, showed a significant relationship with *positive cyber security behaviors*. These results

Table 5: Profile of survey participants

Control	Answer	Freq.	Perc.
Gender (C1)	Male	144	50.7
	Female	140	49.3
	Prefer not to say	0	0.0
	Other	0	0.0
Age (C2)	18–30	68	23.9
	31–50	180	63.4
	> 50	35	12.3
	Prefer not to say	1	0.4
Education (C3)	Primary School	2	0.7
	Secondary/High School	52	18.3
	College/University	230	81.0
Current occupation (C4)	Student	1	0.4
	Employed/Self-employed	271	95.4
	Not employed	9	3.2
	Retired	3	1.1
	Other	0	0.0
Current employee position (C5)	Intern	1	0.4
	Entry-level/Associate	112	39.4
	Manager/Senior manager	147	51.8
	C-level exec./Director/Owner	16	5.6
	Other	8	2.8
Current employee duration (C6)	< half a year	10	3.5
	Between 1/2 year & 2 years	107	37.7
	> than 2 years	167	58.8
Phishing victim (C7)	Yes	129	45.4
	No	155	54.6
Reporting frequency (C8)	Never	45	15.8
	Rarely	49	17.3
	Occasionally	92	32.4
	Frequently	67	23.6
	Always	31	10.9

indicate that higher educated individuals, being part of the organization for a longer period of time, and who consistently report suspicious emails, are also more inclined to perform actions that benefit the cyber security of the organization. Additionally, *Current employment duration*, *Phishing Victim*, and *Reporting frequency* show a significant positive relationship with an individual's *intention to report phishing emails*. This suggests that individuals that are part of the organization for a longer period of time, who fell for phishing emails in the past, and who consistently report suspicious emails, are also more inclined to report phishing emails.

5.2 Questionnaire Reliability and Validity Checks

Reliability. Table 7 shows the internal consistency among the variables measured in our questionnaire. We can observe that Sportsmanship, Altruism, Emotional Stability, Self-efficacy, and Positive Cyber Security Behaviors exceeded the recommended threshold value of 0.7, indicating that the constraint on the internal consistency of these measurements is satisfied. On the other hand, for Extraversion and Subjective Norms we dropped survey items E2, and SN3 respectively (cf. Table 14 in Appendix C), to increase the Cronbach's α value to a value close to the recommended threshold.

Table 6: Relation of controls with Positive Cyber Security Behaviors and Intention to Report

	Control	Pearson correlation	p-value
Positive Cyber Security Behaviors	C1 (Gender)	0.022	0.707
	C2 (Age)	0.046	0.442
	C3 (Education)	0.124*	0.037
	C4 (Current occupation)	-0.113	0.057
	C5 (Current employment position)	0.055	0.360
	C6 (Current employment duration)	0.192**	< 0.001
	C7 (Phishing victim)	0.035	0.552
	C8 (Reporting frequency)	0.527**	< 0.001
Intention to Report	C1 (Gender)	-0.074	0.213
	C2 (Age)	0.079	0.182
	C3 (Education)	0.046	0.440
	C4 (Current occupation)	-0.014	0.820
	C5 (Current employment position)	-0.084	0.157
	C6 (Current employment duration)	0.216**	< 0.001
	C7 (Phishing victim)	-0.137*	0.021
	C8 (Reporting frequency)	0.357**	< 0.001

Correlation is significant at: the 0.01 level (2-tailed), **; the 0.05 level (2-tailed), *

Table 7: Factor Reliability

Factor	Cronbach's α	Observations
Sportsmanship	**0.894**	
Conscientiousness	0.666	
Altruism	**0.777**	
Courtesy	0.658	
Emotional Stability	**0.802**	
Extraversion	0.510	Dropped E2
Self-efficacy	**0.769**	
Subjective Norms	0.673	Dropped SN3
Positive Cyber Sec. Beh.	**0.791**	
Intention to Report	0.693	

For the remaining variables, namely Conscientiousness, Courtesy and intention to report phishing emails, dropping one or more survey items did not have effect on the increase of the internal consistency of the model variables. However, the results show that the Cronbach's α values are always very close to the threshold, leading to an overall satisfactory internal consistency of our measures.

Validity. Table 8 reports the correlations between variables. We can observe that the value of the correlation across all pairs of variables is generally low and below the recommended value of 0.8, indicating no problematic multicollinearity between the considered variables.

5.3 Hypothesis Evaluation

We tested the hypotheses presented in Fig. 1 using the IBM SPSS Statistics software [21]. Fig. 2 presents the results of the regression analysis; coefficients are reported in Table 15 in Appendix D. The figure reports the three models vertically, with plots in the top row containing the standardized coefficients of the human factors without introducing the controls (in blue) and with controls (in red). Plots in the bottom row of Fig. 2 illustrate the standardized coefficients of the controls given the three models. We observe a very small difference between the value of the coefficients of the independent variables when the set of controls is considered compared to when the controls are omitted. As a consequence, the introduced controls do not significantly affect the results of the assessed human factors. Looking at the Adjusted R^2 coefficients reported for the three models in Table 15, we observe a noticeable effect of controls (chiefly, 'C8 - reporting frequency') only on Model 1, for which their addition explains an additional 14% of the variance in the data (from 38% to 52%). This is unsurprising as higher reporting frequencies can be expected to reflect in overall positive cyber security behaviors. By contrast, the addition of controls in Model 1 and Model 2 only contribute to explaining, approximately, an additional one and three percent of variance, respectively (M1: from 42% to 45%; M2: from 54% to 55%). This suggests that the main effects in the model are appropriate to explain reporting intentions, and that no large hidden effects are likely to be found within the controls.

Table 9 reports the hypothesis assessment based on the results of the regression analysis when controls are considered.[3] The standardized β value of each hypothesis represents the value of the variable coefficient assessed in the corresponding model. In terms of human factors, we observe that *Conscientiousness* and *Extraversion* have a positive influence on positive cyber security behaviors, while *Altruism*, *Self-efficacy*, and *Subjective Norms* have a positive effect on the intention to report phishing emails. Additionally, *positive cyber security behaviors* is highly influential on an individual's intention to report phishing emails. Next, we discuss each model individually.

Model 1. Model 1 aims to test whether the selected human factors, namely Sportsmanship, Conscientiousness, Altruism, Courtesy, Emotional Stability and Extraversion, positively affect an individual's positive cyber security behaviors, as captured by hypotheses H1.1 to H1.6. These predictions are partially supported, where Conscientiousness is the most powerful human factor ($\beta = 0.359; p < 0.001$), indicating that conscientious individuals tend to engage in behaviors that are beneficial for the security of the organization. Extraversion is another human factor positively influencing an individual' positive cyber security behaviors ($\beta = 0.122; p = 0.032$), showing that extraverted individuals are inclined to perform helpful behaviors to protect the organization and other employees.

Model 2. Model 2 aims to test whether positive cyber security behaviors positively affect an individual's intention to report phishing emails (H2.1). This prediction is supported, where the intention to report phishing emails is strongly determined by positive cyber security behaviors ($\beta = 0.630; p < 0.001$). This indicates that reporting potentially dangerous emails falls within the behaviors that an individual may perform outside of his organizational tasks and duties.

Model 3. This model hypothesizes that the selected human factors positively affect an individual's intention to report phishing emails (hypotheses H3.1 to H3.8). These hypotheses are partially supported. The results show that beliefs, namely self-efficacy ($\beta = 0.325; p < 0.001$) and subjective norms ($\beta = 0.207; p < 0.001$), are the factors that mostly influence an individual's intention to report phishing

[3]To further verify the robustness of our findings, we re-run all our models adopting a robust OLS regression (which is robust against violations on OLS assumptions) and compared regressed coefficients with those in output of a standard OLS. We find virtually no difference, neither in magnitude nor direction, between the two sets of estimated coefficients for all models.

Table 8: Variable Correlations

Variable	1	2	3	4	5	6	7	8	9	10
1. Sportsmanship	1									
2. Conscientiousness	0.305**	1								
3. Altruism	0.147*	0.554**	1							
4. Courtesy	0.448**	0.632**	0.624**	1						
5. Emotional Stability	0.645**	0.276**	0.164**	0.266**	1					
6. Extraversion	0.177**	0.130*	0.396**	0.161**	0.498**	1				
7. Self-efficacy	0.364**	0.570**	0.552**	0.616**	0.225**	0.193**	1			
8. Subjective Norms	0.147*	0.543**	0.513**	0.556**	0.145*	0.235**	0.520**	1		
9. Positive Cyber Security Behaviors	0.114	0.546**	0.513**	0.463**	0.143*	0.272**	0.541**	0.566**	1	
10. Intention to Report	0.178**	0.544**	0.577**	0 .560**	0.190**	0.206**	0.638**	0.591**	0.651**	1

Correlation is significant at the 0.01 level (2-tailed).**
Correlation is significant at the 0.05 level (2-tailed).*

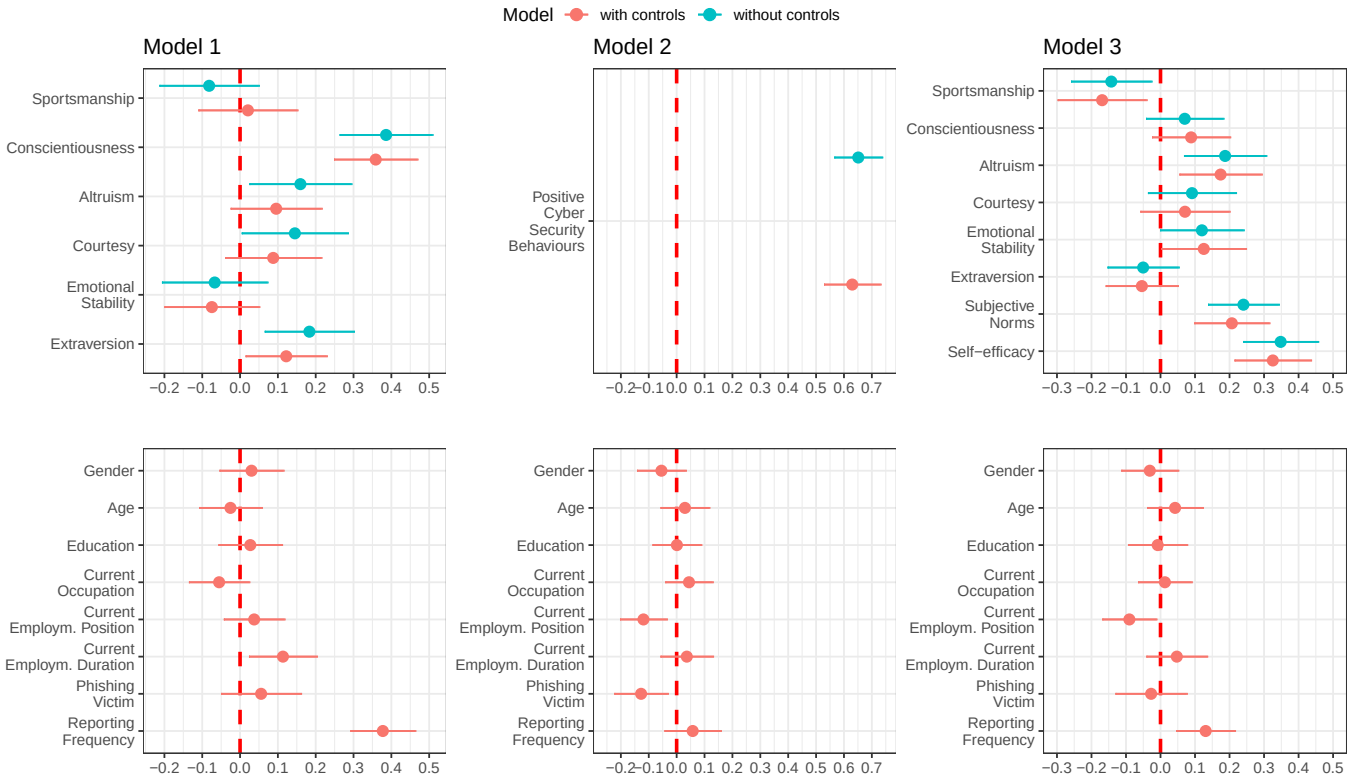

Figure 2: Coefficients of the observed variables and controls

emails. Altruism has also a significant impact on an individual's intention to report phishing emails ($\beta = 0.174; p = 0.006$), showing that altruistic individuals tend to act for the benefit of the organization and their colleagues. Surprisingly, our analysis shows that Sportsmanship has a statistically significant *negative* relationship with the intention to report phishing emails ($\beta = -0.169; p = 0.013$). Individuals with this trait tend to have a high tolerance for less-than-ideal situations such as receiving suspicious emails. In such situations, they might not take further actions to mitigate potential risks and ignore the email, rather than reporting it.

6 DISCUSSION AND IMPLICATIONS

This section presents the theoretical implications of our study and research directions for practice with respect to phishing reporting intentions and positive cyber security behaviors, followed by a discussion on the threats to validity of this study.

6.1 Implications for Theory

This study provides several theoretical implications that can be used in future research, observing the role of cognitive theory in interpreting human behaviors with respect to positive cyber security behaviors within organizations.

Table 9: Hypothesis testing (estimations from models including control variables)

Hypothesis	Human Factor	Standardized β	p-value	Assessment
H1.1	Sportsmanship	0.021	0.763	Not supported
H1.2	Conscientiousness	0.359	< 0.001	Supported
H1.3	Altruism	0.096	0.132	Not supported
H1.4	Courtesy	0.088	0.192	Not supported
H1.5	Emotional Stability	-0.075	0.259	Not supported
H1.6	Extraversion	0.122	0.032	Supported
H2.1	Safe Cyber Security Behaviors	0.630	< 0.001	Supported
H3.1	Sportsmanship	-0.169	0.013	Not supported*
H3.2	Conscientiousness	0.089	0.138	Not supported
H3.3	Altruism	0.174	0.006	Supported
H3.4	Courtesy	0.071	0.298	Not supported
H3.5	Emotional Stability	0.125	0.053	Not supported
H3.6	Extraversion	-0.054	0.327	Not supported
H3.7	Self-efficacy	0.325	< 0.001	Supported
H3.8	Subjective Norms	0.207	< 0.001	Supported

Note: The study results demonstrate a statistically significant negative relationship with the intention to report.

The need for a unified model for phishing reporting behavior: Cyber security behaviors are influenced by both human factors at the individual-level (i.e., OCBI characteristics, personality traits and beliefs) and at organization-level (OCBO characteristics). However, previous work that addressed the two levels have done so only within the OCB characteristics, without considering other influential factors, such as personality traits or beliefs (cf. Table 10).

Comparing results from our findings with prior research underlines the need to develop a cohesive, complete model of reporting behavior to obtain consistent results and derive effective practices. For instance, on the individual level, prior work showed the positive relationship between emotional stability and security assurance/compliance behaviors [11, 42, 43]; by contrast, our study shows that when considered together with other factors, this relationship may not be significant for positive cyber security behaviors. On the other hand, previous work on extraversion reports mixed results across various security behaviors [11, 43] whereas we find a positive relationship with positive cyber security behaviors. These discrepancies can be ascribed to the fact that emotional stability and extraversion have been often studied in isolation and that they might be less relevant when a broader portfolio of human factors (including organization-related) is considered.

At the organizational level (OCBO), previous work has generally positively related cyber security behaviors with the OCB construct [11]; by contrast, our results suggest only conscientiousness (OCBO) is consistent with previous results (if considering also OCBI the divergence is more prominent). Moreover, our finding of a negative relation between sportsmanship and intention to report is unexpected: individuals with high sportsmanship, by definition, can be reasonably expected to be more inclined to 'take one for the team' (referred to, e.g., the nuance of reporting phishing emails) [33]. Unexpectedly, we find the opposite might be true. An interpretation is that high sportsmanship individuals might not want to create additional burden to other 'members of the team' (in this case, those responsible to handle the reports) because of the, in their view, relatively minor inconvenience of receiving a phishing email. The not significant relationship of conscientiousness with intention to report is surprising as well, because previous literature overall reports positive relationships of conscientiousness (from the Big-Five traits) with specific security behaviors like detecting phishing emails [19]. One possible explanation is that individuals with high conscientiousness (as per OCB) may not consider reporting to be within their 'duties' or that reporting is still a concept misunderstood by many [25].

Future research can extend the scope of our study by evaluating the (combined) effects of the other human factors discussed in Section 2.2 as well as of other external factors (e.g., windows of opportunity [14], culture [55]), or factors that can negatively influence reporting. On this line, the bystander effect, i.e., the expectation that others will do the reporting, and the ill-perceived liability of reporting, i.e., the assumption that 'it is the duty of the IT department' to deal with phishing [8], can be valuable avenues for research to extend our model and to build a more comprehensive understanding of reporting behaviors in general.

Generic vs. specific cyber security behaviors: Our evaluation shows a strong positive association between individuals' positive cyber security behaviors and their intention to report phishing emails. This relation indicates that employees who report phishing emails (the *specific* behavior), typically act in accordance with the organization's ISP and exhibit security assurance behaviors (the *generic* behavior). However, our study shows that the underlying human factors driving these behaviors could be different. For instance, our results reveal that sportsmanship and altruism have no strong relationships with the generic positive cyber security behaviors whereas these factors do influence the specific behavior of (intention of) reporting, thus casting doubts on their relation with the generic constructs of SAB and SCB. A possible explanation can be that the latter encompasses behaviors such as 'using password managers' or 'complying with ISP', which poorly align with sportsmanship and altruism. On the other hand, conscientiousness and extraversion appear to have a strong relationship with positive cyber security behaviors, but this does not translate to the specific behavior of reporting. This suggests that relationships between human

traits and *specific* cyber security behaviors do not necessarily translate to *generic* behaviors as one might expect. Therefore, researchers and practitioners should be cautious in applying or generalizing their findings to other types of positive cyber security behaviors.

Future research may investigate the impact that negative security behaviors (i.e., SRB and SDB) [11] may have on the individual's reporting actions. The contrast between positive and negative cyber security behaviors may shift an individual's intention to report, and more specifically, it may alter their perspective on what defines *normal* and *abnormal* behaviors [16]. These security behaviors may reduce the intention to report, while counteracting the effect of the positive cyber security behaviors.

Design of innovative training and awareness programs: Our findings can be used to support the design of innovative training and awareness programs. For example, gamification systems employed in phishing reporting can increase the confidence and motivate individuals to perform beneficial cyber security behaviors [24]. When creating such systems to encourage phishing reporting, human factors shaping cyber security behaviors may serve as instruments for fine-tuning the users' interactions with such a system (e.g., the number of false positives may increase when employees are prompted to reporting hits). Our findings suggest that building the employees' confidence in their capability to report potential attacks and the perceived validation from authoritative sources may also increase the individual's motivation to engage in beneficial cyber security behaviors and comply with the organization's policy.

6.2 Research Directions for Practice

Our findings also point at interesting research directions to investigate novel approaches for training and awareness programs that organizations often provide, as well as aiming at improving the organizational culture and the overall security posture of an organization (cf. Section 2).

Training: This study provides insights relevant to the design of training practices aimed at improving reporting behavior. For example, our study suggests that high sportsmanship is linked to low intention to report a suspicious email. As high-sportsmanship individuals may tend to avoid creating additional work to others because of their own negative experiences, a training program may want to 'fight back' this effect by explicitly gearing the training towards minimizing the negative effects of reporting (i.e., the filed 'complaint') creates on the organization, and maximizing the relevance of the positive outcome in terms of increased overall security. For example, regular training programs aimed at training phishing detection could be extended to cover the process by which reported emails are handled by dedicated staff and to provide hard-data on the outcomes of the reporting process. Similarly, feedback mechanisms informing the reporter of the effects of their report may help in curtailing the negative effect measured for high sportsmanship individuals. On a similar line, we find self-efficacy and subjective norms to be also factors positively related to the intention to report phishing emails. These findings indicate, for instance, that training programs should focus on the reporting mechanisms as well, rather than (primarily) on the detection of phishing attacks, and employ special interventions aimed at enhancing employees' self-efficacy in this direction. Additional research in this direction is needed to evaluate the effects that these human factors have on training effectiveness.

Awareness: This study's outcomes can also point to future directions to improve the efficacy of cyber security awareness programs. For example, awareness programs can explicitly acknowledge the contribution of conscientious behaviors to support the organization's security posture and reward diligent individuals to motivate them and inspire others to maintain it. Therefore, incentive programs or approaches can be introduced to encourage employees to exceed the formal expectations of the organization, while increasing their awareness of data security. Similarly, employees' altruistic tendencies can be accounted for in awareness programs to encourage the reporting of phishing attacks; for example, awareness programs could further clarify why such behaviors benefit the organization as a whole, and how they can contribute to protecting colleagues that might not be as skilled in recognizing phishing attacks. These insights could be integrated into awareness programs by different means, for example by targeting 'tailored' programs to specific groups or by explicitly acknowledging the role of the single employee in protecting their peers.

Culture: The organization's collective assumptions, values, and perceptions can be a valuable tool to mold positive cyber security behaviors [6]. With respect to phishing reporting behavior, our findings suggest that fostering an organization's culture to encourage individual initiative (self-efficacy) and promote clear expectations within the work environment (subjective norms) may have beneficial effects on reporting and, more in general, on positive cyber security behaviors [35]. The recognition as a cultural value of a conscientious commitment to cyber security and, thus, to the overall well-being of the organization's collective can boost the motivation of individuals to 'keep up the good work'. Moreover, cherishing individual openness and activeness, often observed in extravert individuals, can be an untapped resource for attack mitigation to improve the security posture of the organization. Similarly, altruistic behaviors may be emphasized when defining the organizational culture, where such behaviors are accepted as the norm, and peer collaboration is promoted. Encouraging these behaviors would also lead to a positive outcome for taking protective actions, such as reporting potential phishing attacks. Employees can act as a collective phishing detection mechanism, even in large organizations, enabling fast detection and thwarting of new phishing campaigns with acceptable operational load [31]. Such a mitigation strategy can be 'embedded' in the organization's security stance by developing a sustainable security culture, for example, as part of the organizational culture itself.

6.3 Threats to Validity

Construct Validity. The study evaluates an individual's intention to report and not the actual reporting behavior. As a consequence, the construct addressed in the paper may not be sufficient to assess reporting behaviors. However, several theories such as PMT [50] and TPB [1] show there is a close relationship between intention and actual behavior and that measures of intention are widely accepted as indicators for actual behaviors.

Internal Validity. To evaluate the internal validity of the study, we assess the measures used for the theoretical model and the conducted

survey. Firstly, the reliability of the model is generally supported by satisfactory Cronbach's α values (cf. Table 7). On the other hand, some constructs (chiefly, extraversion, and to a lesser extent conscientiousness, courtesy, subjective norms, and intention to report) do show lower internal consistency levels; however, our attempts to increase consistency by removing items to the questionnaires did not help for those constructs, despite being directly adapted from survey questions adopted in the literature [11, 15, 44, 53]. Future work could address how to design more robust measurements for those constructs. Secondly, the sample size for the survey participants is adequate, as the minimum sample size required to assess the outcome is achieved. Finally, we employed several checks to ensure the validity of the survey responses used in the analysis (cf. Section 4.1). The collected data, however, might be affected by other bias. For instance, we based the survey items used to measure human factors on existing assessment methods. These survey items are in the form of agree–disagree questions, which can lead to acquiescence response bias [32]. This bias can influence the survey data, where respondents may have the tendency to agree with the questions presented. Future research might design construct-specific questions to mitigate this type of bias [29].

External Validity. To determine the minimum sample size to achieve an acceptable precision in the analysis, we employed a sample size estimation calculation, as described in Appendix B. For our study, we recruited participants located in the US through AMT. While it has been shown that AMT workers in the US are representative of the US population when performing security- and privacy-related tasks [48], our results may not generalize to other populations. On the other hand, the respondent demographics reported in Table 5 seem to show relatively high rates of phishing victimization rate and high professional seniority. A possible explanation is that the type of task focused on phishing in organizations attracted users with previous experience on the topic. Given that the reference population for our study consists of employed professionals exposed to phishing emails, we consider our findings applicable to that population. The experiment can be reproduced, with respondents from various countries and different levels of email use experience, to minimize the effect of the selection bias and estimate whether different interpretations of the intention to report phishing emails exist.

7 CONCLUSION

In this study, we investigated the influence of human factors on an individual's intention to report phishing emails. To this end, we developed a theoretical model of human factors and their relations with an individual's positive cyber security behaviors and intention to report phishing emails. We evaluated the model through an experiment within Amazon Mechanical Turk, where 284 participants answered an online survey. The results show that there exists a strong relationship between an individual's positive cyber security behaviors (security assurance and security compliance behaviors) and his intention to report phishing emails. Moreover, among the studied human factors, we observed that self-efficacy, subjective norms, and altruism positively impact reporting intention. However, the results reveal that sportsmanship hinders an individual's intention to report phishing emails. Although this work sheds the light on theoretical and practical implications of human factors in the InfoSec context, more research and experiments are required to evaluate how human factors can be exploited to improve an organization's training and awareness programs as well as to foster an organization's culture that promotes positive cyber security behaviors.

Acknowledgment. This work is supported by the ITEA3 programme through the DEFRAUDIfy project funded by Rijksdienst voor Ondernemend Nederland (grant no. ITEA191010) and by the INTERSCT project, Grant No. NWA.1162.18.301, funded by Netherlands Organisation for Scientific Research (NWO).

REFERENCES

[1] Icek Ajzen. 1991. The theory of planned behavior. *Organizational Behavior and Human Decision Processes* 50, 2 (1991), 179–211.
[2] Luca Allodi, Tzouliano Chotza, Ekaterina Panina, and Nicola Zannone. 2020. The Need for New Antiphishing Measures Against Spear-Phishing Attacks. *IEEE Security Privacy* 18, 2 (2020), 23–34.
[3] Kholoud Althobaiti, Adam D G Jenkins, and Kami Vaniea. 2021. A Case Study of Phishing Incident Response in an Educational Organization. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2, Article 338 (2021), 32 pages.
[4] Teresa Amabile, Elizabeth Schatzel, Giovanni Moneta, and Steven Kramer. 2004. Leader Behaviors and the Work Environment for Creativity: Perceived Leader Support. *The Leadership Quarterly* 17 (2004), 5–32.
[5] Amazon. 2022. *Amazon Mechanical Turk.* Retrieved September 12, 2022 from https://www.mturk.com/
[6] Gaurav Bansal. 2018. Got Phished! Role of Top Management Support in Creating Phishing Safe Organizations. *MWAIS 2018 Proceedings* (2018).
[7] Murray R. Barrick and Michael K. Mount. 1991. The Big Five Personality Dimensions and Job Performance A Meta-Analysis. *Personnel Psychology* 44, 1 (1991), 1–26.
[8] Pavlo Burda, Luca Allodi, and Nicola Zannone. 2020. Don't Forget the Human: a Crowdsourced Approach to Automate Response and Containment Against Spear Phishing Attacks. In *European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 471–476.
[9] Marcus Butavicius, Kathryn Parsons, Malcolm Pattinson, and Agata McCormac. 2015. Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails. *ACIS 2015 Proceedings* 98 (2015), 11.
[10] Robert Colosi. 2005. Negatively Worded Questions Cause Respondent Confusion. *Proceedings of the Survey Research Methods Section* (2005), 2896–2903.
[11] Rachel Christine Dreibelbis. 2016. It's More Than Just Changing Your Password: Exploring the Nature and Antecedents of Cyber-Security Behaviors. *USF Tampa Graduate Theses and Dissertations* (2016).
[12] FBI Internet Crime Complaint Centre. 2020. *Internet Crime Report 2020.*
[13] R. A. Fisher. 1992. Statistical Methods for Research Workers. In *Breakthroughs in Statistics: Methodology and Distribution.* Springer, New York, NY, 66–70.
[14] A.V. Gershman, J.F. McCarthy, and A.E. Fano. 1999. Situated computing: bridging the gap between intention and action. In *International Symposium on Wearable Computers.* IEEE, 3–9.
[15] Lewis R. Goldberg. 1999. A broad-bandwidth, public-domain, personality inventory measuring the lower-level facets of several five-factor models. *Personality Psychology in Europe* 7 (1999), 7—-28.
[16] Ken H. Guo. 2013. Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security* 32 (2013), 242–251.
[17] Kim Jong Hae. 2019. Multicollinearity and misleading statistical results. *Korean J Anesthesiol* 72, 6 (2019), 558–569.
[18] Tzipora Halevi, Nasir Memon, James Lewis, Ponnurangam Kumaraguru, Sumit Arora, Nikita Dagar, Fadi Aloul, and Jay Chen. 2016. Cultural and Psychological Factors in Cyber-Security. In *International Conference on Information Integration and Web-based Applications & Services.* ACM, New York, NY, USA, 43–56.
[19] Tzipora Halevi, Nasir Memon, and Oded Nov. 2015. *Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks.* SSRN Scholarly Paper. Social Science Research Network. https://doi.org/10.2139/ssrn.2544742
[20] Graeme D Hutcheson. 2011. Ordinary least-squares regression. In *The SAGE dictionary of quantitative management research.* SAGE Knowledge, 224–228.
[21] IBM Corp. [n. d.]. *IBM SPSS Statistics for Windows.*
[22] Nadim Jahangir, Mohammad Muzahid Akbar, and Mahmudul Haq. 2004. Organisational Citizenship Behavior: Its Nature and Antecedents. *BRAC University Journal* 1, 2 (2004), 75–85.
[23] Mohammad S. Jalali, Maike Bruckes, Daniel Westmattelmann, and Gerhard Schewe. 2020. Why Employees (Still) Click on Phishing Links: Investigation in Hospitals. *Journal of Medical Internet Research* 22, 1 (2020), e16775.

[24] Matthew L. Jensen, Ryan T. Wright, Alexandra Durcikova, and Shamya Karumbaiah. 2022. Improving Phishing Reporting Using Security Gamification. *Journal of Management Information Systems* 39, 3 (2022), 793–823.

[25] Leon Kersten, Pavlo Burda, Luca Allodi, and Nicola Zannone. 2022. Investigating the Effect of Phishing Believability on Phishing Reporting. In *European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 117–128.

[26] Sabina Kleitman, Marvin K. H. Law, and Judy Kay. 2018. It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling. *PLOS ONE* 13, 10 (2018), 1–29.

[27] P. Kline. 1993. *The Handbook of Psychological Testing (2nd ed.)*. Routledge. 66–70 pages.

[28] Igor Knez, Daniel Hjärpe, and Mari Bryngelsson. 2019. Predicting Organizational Citizenship Behavior: The Role of Work-Related Self. *SAGE Open* 9 (2019), 215824401985483.

[29] Jon A. Krosnick and Stanley Presser. 2010. Question and questionnaire design. In *Handbook of survey research*. Emerald, 263–314.

[30] Youngsun Kwak, Seyoung Lee, Amanda Damiano, and Arun Vishwanath. 2020. Why Do Users Not Report Spear Phishing Emails? *Telematics and Informatics* 48 (2020), 101343.

[31] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. 2022. Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. In *Symposium on Security and Privacy*. IEEE, 842–859.

[32] Yphtach Lelkes and Rebecca Weiss. 2015. Much ado about acquiescence: The relative validity and reliability of construct-specific and agree–disagree questions. *Research & Politics* 2, 3 (2015).

[33] Jeffrey LePine, Amir Erez, and Diane Johnson. 2002. The Nature and Dimensionality of Organizational Citizenship Behavior: A Critical Review and Meta-Analysis. *The Journal of applied psychology* 87 (2002), 52–65.

[34] Jeovany Martínez-Mesa, David González-Chica, João Bastos, Renan Bonamigo, and Rodrigo Duquia. 2014. Sample size: how many participants do I need in my research? *Anais brasileiros de dermatologia* 89 (2014), 609–615.

[35] Peter Mayer, Alexandra Kunz, and Melanie Volkamer. 2017. Reliable Behavioural Factors in the Information Security Context. In *International Conference on Availability, Reliability and Security*. ACM, New York, NY, USA, Article 9, 10 pages.

[36] Robert R. McCrae and Paul T. Costa. 1987. Validation of the Five-Factor Model of Personality Across Instruments and Observers. *Journal of Personality and Social Psychology* 52, 1 (1987), 81–90.

[37] Rosana Montañez, Edward Golob, and Shouhuai Xu. 2020. Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology* 11 (2020).

[38] Tjai M. Nielsen, Daniel G. Bachrach, Eric Sundstrom, and Terry R. Halfhill. 2012. Utility of OCB: Organizational Citizenship Behavior and Group Performance in a Resource Allocation Framework. *Journal of Management* 38, 2 (2012), 668–694.

[39] W. T. Norman. 1963. Toward an adequate taxonomy of personality attributes: replicated factors structure in peer nomination personality ratings. *Journal of abnormal and social psychology* 66 (1963), 574–583.

[40] Dennis Organ. 1997. Organizational Citizenship Behavior: It's Construct Clean-Up Time. *Human Performance* 10 (1997), 85–97.

[41] Dennis W Organ. 1988. *Organizational citizenship behavior: The good soldier syndrome*. Lexington Books/DC Heath and Com.

[42] Kathryn Parsons, Agata McCormac, Malcolm Pattinson, Marcus Butavicius, and Cate Jerram. 2013. Phishing for the Truth: A Scenario-Based Experiment of Users' Behavioural Response to Emails. In *Security and Privacy Protection in Information Processing Systems (IFIP Advances in Information and Communication Technology)*. Springer, 366–378.

[43] Malcolm Pattinson, Cate Jerram, Kathryn Parsons, Agata McCormac, and Marcus Butavicius. 2012. Why do some people manage phishing e-mails better than others? *Information Management & Computer Security* 20, 1 (2012), 18–28.

[44] Philip M. Podsakoff, Scott B. MacKenzie, Robert H. Moorman, and Richard Fetter. 1990. Transformational leader behaviors and their effects on followers' trust in leader, satisfaction, and organizational citizenship behaviors. *The Leadership Quarterly* 1, 2 (1990), 107–142.

[45] Samuel Pond III, Rupert Nacoste, Monique Mohr, and Christopher Rodriguez. 2006. The Measurement of Organizational Citizenship Behavior: Are We Assuming Too Much? *Journal of Applied Social Psychology* 27 (2006), 1527–1544.

[46] Clay Posey, Tom L. Roberts, and Paul Benjamin Lowry. 2015. The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems* 32, 4 (2015), 179–214.

[47] Elissa M. Redmiles, Yasemin Gülsüm Acar, Sascha Fahl, and Michelle L. Mazurek. 2017. *A Summary of Survey Methodology Best Practices for Security and Privacy Researchers*. Technical Reports of the Computer Science Department CS-TR-5055. University of Maryland.

[48] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2019. How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples. In *Symposium on Security and Privacy*. IEEE, 1326–1343.

[49] Sandra L. Robinson. 1996. Trust and Breach of the Psychological Contract. *Administrative Science Quarterly* 41 (1996), 574–599.

[50] Ronald W. Rogers. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change1. *The Journal of Psychology* 91, 1 (1975), 93–114.

[51] Noor Romaiha, Fatin Maulud, Wan Musyirah, Arnida Jahya, Nurul Fahana, and Aini Harun. 2019. The Determinants of Organizational Citizenship Behaviour (OCB). *International Journal of Academic Research in Business and Social Sciences* 9 (2019), 124—-133.

[52] Edgar Schein. 2010. *Organizational Culture and Leadership*. Jossey-Bass.

[53] Hamidreza Shahbaznezhad, Farzan Kolini, and Mona Rashidirad. 2020. Employees Behavior in Phishing Attacks What Individual Organizational and Technological Factors Matter. *Journal of Computer Information Systems* 61, 6 (2020), 539–550.

[54] Steve Sheng, Mandy Lanyon, Ponnurangam Kumaraguru, Lorrie Cranor, and Julie Downs. 2010. Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. In *SIGCHI Conference on Human Factors in Computing Systems*. ACM, New York, NY, USA, 373–382.

[55] Mikko Siponen, M. Adam Mahmood, and Seppo Pahnila. 2014. Employees' adherence to information security policies: An exploratory field study. *Information & Management* 51, 2 (2014), 217–224.

[56] Barbara Sypniewska. 2020. Counterproductive Work Behavior and Organizational Citizenship Behavior. *Advances in Cognitive Psychology* 16 (2020), 321–328.

[57] Jenny Tang, Eleanor Birrell, and Ada Lerner. 2022. Replication: How Well Do My Results Generalize Now? The External Validity of Online Privacy and Security Surveys. In *Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Boston, MA, 367–385.

[58] US Department of Labor. 2022. *Minimum wage*.

[59] Wade M. Vagias. 2006. *Likert-Type Scale Response Anchors*. Technical Report. Clemson University.

[60] Verizon. 2021. *2021 Data Breach Investigations Report*.

[61] Verizon. 2022. *2022 Data Breach Investigations Report*.

[62] Bas Verplanken, Henk Aarts, Ad van Knippenberg, and Anja Moonen. 1998. Habit versus planned behaviour: A field experiment. *British Journal of Social Psychology* 37, 1 (1998), 111–128.

[63] Arun Vishwanath. 2015. Examining the Distinct Antecedents of E-Mail Habits and its Influence on the Outcomes of a Phishing Attack. *Journal of Computer-Mediated Communication* 20, 5 (2015), 570–584.

[64] Arun Vishwanath, Tejaswini Herath, Rui Chen, Jingguo Wang, and H. Raghav Rao. 2011. Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems* 51, 3 (2011), 576–586.

[65] Larry J. Williams and Stella E. Anderson. 1991. Job Satisfaction and Organizational Commitment as Predictors of Organizational Citizenship and In-Role Behaviors. *Journal of Management* 17, 3 (1991), 601–617.

[66] Ryan Wright and Kent Marett. 2010. The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived. *Journal of Management Information Systems* 27 (2010), 273–303.

Table 10: Construct correlations between human factors and cyber security behaviors from previous studies

Construct	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1. Civic Virtue	-																				
2. Leader Support	-.08 [33]	-																			
3. Organizational Commitment	.03 [33]	-	-																		
4. Sportsmanship	.045** [33]	-.02 [33]	-.04 [33]	-																	
5. Conscientiousness (OCB)	.035** [33]	-.03 [33]	.01 [33]	.019 [33]	-																
6. Job satisfaction	.01 [33]	-	.44** [45]	.03 [33]	.00 [33]	-															
7. Altruism	.023** [33]	.35** [33]	.21** [33]	.048** [33]	.037** [33]	.23** [33]	-														
8. Courtesy	.012** [33]	-.02 [33]	-.06 [33]	.046** [33]	.023** [33]	.02 [33]	.031** [33]	-													
9. Agreeableness	-	-	-	-	-	-	-	-	-												
10. Conscientiousness (Big Five)	-	-	-	-	-	-	-	-	.39*** [11]	-											
11. Openness to Experience	-	-	-	-	-	-	-	-	.35*** [11]	.33*** [11]	-										
12. Extraversion	-	-	-	-	-	-	-	-	.30*** [11]	.11* [11]	.22*** [11]	-									
13. Emotional Stability	-	-	-	-	-	-	-	-	-	-	-	-	-								
14. (Email) Habits	-	-	-	-	-	-	-	-	-	-	-	-	-	-							
15. Subjective Norms	-	-	-	-	-	-	-	-	-	-	-	-	-	.76 [53]	-						
16. Self-efficacy	-	-	-	-	-	-	-	-	-	-	-	-	-	.77 [53]	.59 [53]	-					
17. OCBO	-	.03 [33]	-.02 [33]	-	.03 [33]	.01 [33]	.42*** [11]	-	.42*** [11]	.48*** [11]	.29*** [11]	-.02 [11]	.27*** [11]	-	-	-	-				
18. OCBI	-	.30** [33]	.21** [33]	-	.22** [33]	.24** [33]	.36*** [11]	-	.36*** [11]	.35*** [11]	.29*** [11]	.13** [11]	.08 [11]	-	-	-	.34*** [11]	-			
19. OCB	.37 [38]	.41** [33]	.32** [33]	.51** [38]	.13 [33]	.31** [33]	-	-	-	-	-	-	-	-	-	-	-	-	-		
20. SAB	-	-	-	-	-	-	-	-	.15** [11]	.18** [11]	.11* [11]	.07 [11]	.19*** [11]	-	-	-	.15*** [11]	.18*** [11]	-	-	
21. SCB	-	-	-	-	-	-	-	-	.29*** [11]	.27*** [11]	.27*** [11]	.03 [11]	.21*** [11]	-	-	-	.44*** [11]	.22*** [11]	-	.25*** [11]	-

with: $^{*}p \leq .05$, $^{**}p \leq .01$, $^{***}p \leq .001$

APPENDIX

A CONSTRUCT CORRELATION VALUES EXTRACTED FROM LITERATURE

Table 10 reports the construct correlation values from the literature.

B SAMPLE SIZE CALCULATIONS

We performed the Fisher's Exact Test [13] on the pilot data to observe which controls, from the selected list of eight controls, needed to be considered for calculating the sample size. The resulted p-values from this test, assessing the statistical significance of each control with the intention to report, are presented in Table 11. We considered controls with $p \leq 0.05$ as statistically *significant*, and p-values higher than 0.05 but $p \leq 0.1$ as *borderline significant*. Therefore, the selected controls, with a maximum p-value of 0.052, were: Education ($p = 0.002$), Phishing victim ($p = 0.003$), Current employment position ($p = 0.052$), and Reporting frequency ($p =< 0.001$). Table 12 presents the calculated parameters, as well as the computed minimum sample size, predicted from the data gathered from the pilot. The resulting maximum value for the minimum sample size was $n = 267$.

Table 11: p-value of Controls in relationship with the Intention to Report observed in the survey

Control	Intention to report: p-value
Gender	0.397
Age	0.852
Education	0.002
Current occupation	0.330
Current employment position	0.052
Current employment duration	0.388
Phishing victim	0.003
Reporting frequency	< 0.001

Table 12: Sample size calculation

Exposure	**Outcome Prevalence**		
	Intention to report phishing pO = 62 %		
		Exp. PR 1.50	Exp. PR 2.00
Education	**Power**	**PONE: 45%**	**PONE: 35.3%**
College/Univ.:75.8% (E)	80%	n = 200	n = 82
Other: 24.2% (NE)	90%	n = 267	n = 109
r: 0.32			
Employment position	**Power**	**PONE: 50.5%**	**PONE: 42.6%**
Manag./Sen. manag.:45.5% (E)	80%	n = 118	n = 42
Other: 54.5% (NE)	90%	n = 158	n = 57
r: 1.2			
Phishing victim	**Power**	**PONE: 55.3%**	**PONE: 49.9%**
Yes: 24.2% (E)	80%	n = 132	n = 41
No: 75.8% (NE)	90%	n = 177	n = 56
r: 3.13			
Reporting frequency	**Power**	**PONE: 57.9%**	**PONE: 54.3%**
Always: 14.1% (E)	80%	n = 183	n = ND
Other: 85.9% (NE)	90%	n = 245	n = ND
r: 6.1			

Note: ND = value could not be determined, as prevalence of outcome in the exposed would be above 100%, according to the specified parameters.

C QUESTIONNAIRE

Table 13 presents the questions to gather participants' demographic information, and Table 14 presents the survey item. For each constructs, the latter table reports the hypotheses and the corresponding characteristics, along with which survey items measure the selected characteristics, and the study which served as reference.

Table 13: Demographic questions in the survey

No.	Demographic Question	Answer Options
C1	What is your gender?	Male Female Prefer not to say Other
C2	What is your age in years?	Young adult (18–30) Adult (31–50) Senior adult (> 50) Prefer not to say
C3	What is the highest degree or level of school you have completed? If currently enrolled, please select the highest degree you have already completed.	Primary School Secondary/High School College/University
C4	Which of the following categories best describes your current position, if any? Note: If 'Not employed' or 'Retired' is selected, please consider your affiliation with the last organization when answering the upcoming questions.	Student Employed/Self-employed Not employed Retired Other, please specify
C5	Which of the following categories best describes your employment position/role at the organization you are affiliated with?	Intern Entry-level/Associate Manager/Senior manager C-level executive/Director/Owner Other, please specify
C6	For how long have you been in your selected position regarding the previously mentioned affiliation with the organization?	Less than half a year Between half a year and 2 years More than 2 years
C7	As far as you know, have you ever fallen for a fraudulent phishing email?	Yes No
C8	When you receive an email in your inbox that you consider suspicious, how often do you report it?	Never Rarely Occasionally Frequently Always

Table 14: Survey items

Hypothesis	Characteristic	Survey Item	Reference
Part I			
H1.5, H3.5	Emotional Stability	At my workplace… *(ES1)* I am relaxed most of the time. *(ES2)* I often feel sad/discouraged. (R) *(ES3)* I get stressed out easily. (R) *(ES4)* I worry about things. (R)	[15]
H1.6, H3.6	Extraversion	At my workplace… *(E1)* I feel comfortable around my co-workers. *(E2)* I do not mind being the center of attention. *(E3)* I do not talk a lot with my co-workers. (R) *(E4)* I do not like to draw attention to myself. (R)	[15]
H1.1, H3.1	Sportsmanship	*(S1)* I spend a lot of time complaining about trivial matters to my co-workers. (R) *(S2)* I always focus on what is wrong at work, rather than the positive side. (R) *(S3)* I tend to make problems seem worse than they actually are. (R) *(S4)* I criticize/find fault in what the organization is doing. (R)	[44]
H1.2, H3.2	Conscientiousness	*(CNS1)* I treat my punctuality at work with seriousness. *(CNS2)* I take no undeserved breaks at work. *(CNS3)* I follow the organization's informal rules and policies, even when no one is watching. *(CNS4)* I am committed to diligently putting in the amount of work expected by my employer.	[44]
H1.3, H3.3	Altruism	*(A1)* I assist my co-workers with their tasks when they have been absent or have heavy workloads. *(A2)* I go out of my way to help new co-workers within the organization. *(A3)* I willingly lend a compassionate ear to co-workers who have work-related or personal problems. *(A4)* I willingly lend a helping hand to the co-workers around me when they need me.	[44]
H1.4, H3.4	Courtesy	*(CO1)* I take steps to try and prevent creating problems for other employees (i.e., changing holiday schedule / work days / shifts). *(CO2)* I am mindful of how my behavior affects my co-workers' jobs. *(CO3)* I do not abuse the rights of my co-workers. *(CO4)* I consider the impact of my actions on my co-workers.	[44]
Part II			
H3.7	Self-efficacy	*Scenario:* You are part of Western University, an institution which encourages employees to follow their strongly defined data policies and regulations that aim at protecting the organization's private data. John works as an HR advisor within the Human Resources Management department of the Western University. This university has a strong Information Security Policy that requires stringent compliance with email security requirements. This policy requires that suspicious emails must be reported to the Information Security department of the university. Due to this role in the university, John sends and receives numerous emails on a regular basis from job agencies, as well as from possible job candidates. One such received email from a trusted job agency contained cues that made John suspicious that the email could be a phishing email. He contacted the job agency in order to warn them about the possibility of them being impersonated by an attacker in a phishing incident. However, considering that he could recognize the email as phishing, John did not value it as a high-risk threat. Therefore, he did not report it to the university's Information Security department, and simply deleted it from his inbox.	[53]

…continued

Hypothesis	Characteristic	Survey Item	Reference
		(SE1) I am confident that if I find myself in John's position, I would be able to contact the job agency about the suspicious email. *(SE2)* I am confident that I am able to report by myself an email that I found to be suspicious. *(SE3)* At this moment, I am confident that I am able to report an email I find suspicious, even if there was no one around to tell me what to do. *(SE4)* At this moment, I am confident that I am able to report an email I find suspicious, if I could ask for help when I am stuck.	
H3.8	Subjective Norms	I believe that… *(SN1)* my supervisors think that I should put effort into protecting the private data of the organization. *(SN2)* my colleagues think that protecting the private data of the organization is our responsibility. *(SN3)* my supervisors think that I should increase my performance at work, and to do so, I overlook/omit the obligations I have for protecting the private data of the organization. (R) *(SN4)* my organization's IT department thinks that I must follow the Information Security policies.	[53]
H2.1	Positive Cyber Security Behaviors	*(POS1)* I monitor my work computer for signs of a virus and/or malware. *(POS2)* I immediately report suspicious emails I receive at work after reading them. *(POS3)* I go above and beyond what is required of me in order to protect the private data of the organization. *(POS4)* I follow the Information Security Policies and practices of the organization I work for. *(POS5)* I use the Information Security technology provided to me by the organization I work for. *(POS6)* I comply with organizational Information Security Policies in order to protect the organization's Information Systems.	[11]
Part III			
	Intention to Report Phishing Emails	I believe that reporting suspicious emails to the organization's IT department may be desirable because… *(REP1)* it is required by the email security policy of the organization I work for. *(REP2)* it is important to contribute to protecting the organization that I work for as a whole. *(REP3)* it is important to contribute to protecting the information and technology resources of the organization I work for. *(REP4)* it is important to contribute to protecting my colleagues from similar attacks.	
		Open question: Is there any remark you would like to make on why anybody, you included, may or may not want to report phishing emails?	-
	Attention check:	This is an attention check question, so please click on the answer 'Occasionally'.	

Notes: R = reverse scored question

D REGRESSION ANALYSIS RESULTS

Table 15: Linear Regression Results

Group	Factor	Model 1 DV: $PCSB(Ui)$		Model 2 DV: $RepInt(Ui)$		Model 3 DV: $RepInt(Ui)$	
OCBO	**Sportsmanship**	-.082	.021			-.143*	-.169*
	Conscientiousness	.386***	.359***			.070	.089
OCBI	**Altruism**	.160*	.096			.187**	.174**
	Courtesy	.145†	.088			.091	.071
Pers. Attr.	**Emotional Stability**	-.067	-.075			.120†	.125†
	Extraversion	.183**	.122*			-.050	-.054
Beliefs	**Self-efficacy**					.348***	.325***
	Subjective Norms					.240***	.207***
	Positive Cyber Sec Behaviors			.651***	.630***		
Controls	**C1 (Gender)**		.030		-.055		-.031
	C2 (Age)		-.025		.030		.042
	C3 (Education)		.027		.001		-.008
	C4 (Current occupation)		-.055		.044		.013
	C5 (Current empl. position)		.037		-.119**		-.090*
	C6 (Current empl. duration)		.113*		.036		.047
	C7 (Phishing victim)		.056		-.127*		-.027
	C8 (Reporting frequency)		.377***		.058		.131**
	Adjusted R^2	.378	.521	.422	.455	.535	.549
	F	29.636	22.959	207.765	27.207	41.762	22.504
	$Obs.$	284	284	284	284	284	284

$^{\dagger}p \leq .1$
$^{*}p \leq .05$
$^{**}p \leq .01$
$^{***}p \leq .001$