What Makes Phishing Simulation Campaigns (Un)Acceptable? A Vignette Experiment on the Acceptance and Manipulation Intention related to Phishing Simulation Campaigns

ANONYMOUS AUTHOR(S)*

Organizations depend on their employees' long-term cooperation to protect themselves from threats. The acceptance of cybersecurity training measures is thus crucial. Phishing attacks are the point of entry for harmful follow-up attacks, and many organizations use simulated phishing campaigns to train employees to adopt secure behaviors. We conducted a pre-registered vignette experiment (N=793)[1], investigating the factors that make a simulated phishing campaign seem (un)acceptable, and their influence on intention to manipulate the campaign. In an online experiment, we varied whether employees gave prior consent, whether the phishing email promised a financial incentive and the consequences for employees who clicked on the phishing link. We found that employees' prior consent had a positive effect on the acceptance of a simulated phishing campaign. The consequences "employee interview" and "termination of the work contract" had a negative effect on acceptance. We found no statistically significant effects of consent, monetary incentive, and consequences on manipulation probability. Few participants described reasons for "manipulating" the campaign, mainly mentioning curiosity. Our results shed light on the factors influencing acceptance of simulated phishing campaigns and provide take-aways for future work in this space.

CCS Concepts: • **Security and privacy** → **Usability in security and privacy**; • **Human-centered computing** → **Empirical studies in HCI**.

Additional Key Words and Phrases: Phishing emails, Acceptance, Between-subjects experiment

1 INTRODUCTION

Organizations rely heavily on email for both internal and external communication and are thus highly vulnerable to phishing attacks. Phishing describes an attack to obtain personal or confidential information from the victim through a message (e.g., an e-mail) by deliberately deceiving them and tricking them into harmful actions [12, 54]. Organizations that fall for phishing attacks face a number of serious consequences. Potential harms include personal damage to the person who interacted with a phishing email and their contacts, financial loss to individuals and organizations [28], harm to infrastructure such as power outages[13, 35], and subsequent societal impact such as problems with public infrastructure that relies on electricity to function (e.g., hospitals).

Phishing is inherently an issue involving human and technical aspects. Technical phishing detection plays an important role in phishing protection, for instance, by preventing phishing emails from making it to a target's inbox. The main technical strategies for phishing detection include blocking known phishing URLs and taking down (removing) known landing pages [54]. Other options include checking whether websites include certain characteristics that could be associated with phishing and page similarity detection [55]. A limitation of many technical phishing mitigations is that they often work best when many similar emails are sent to many potential victims. Technical solutions often cannot protect the first person(s) who are exposed to a certain attack [49]. Technical detection is also difficult in the case of highly targeted phishing attacks ("spear-phishing" [55]). Such attacks typically involve previous research and include personal information of the target.

Many attacks cannot be filtered out through technical means. Organizations thus involve employees to protect the organizations from phishing attacks, such as raising awareness of phishing and training [11] and cybersecurity incident

[1] Pre-registration link: https://osf.io/ew852/?view_only=5717db18d55e46e9a63ff1e050c9aa55

reporting [6]. In organizational contexts, employee acceptance of phishing countermeasures is crucial since simulated phishing campaigns are one of the available training opportunities. In such simulated campaigns, organizations send "realistic" phishing attacks to their own employees, often for training or evaluation purposes [11, 18]. Several commercial vendors conduct such simulated phishing campaigns as a service, providing a user-friendly interface to conduct the simulated campaign and analyze the results. Typically, if an employee interacts with the phishing email (clicks on a link, downloads an attachment), they are then re-directed to a training website explaining the indicators of phishing emails [18]. In some organizations, there are additional consequences for employees who interact with a simulated phishing email. These range from obligatory training to having a conversation about cybersecurity, or in extreme cases, disciplinary consequences [23, 27].

Employee acceptance of simulated phishing campaigns is fundamental for several reasons, including reputation loss, employee attrition, loss of trust in the employer, and maladaptive behaviors [7]. Employees who are subjected to simulated phishing campaigns sometimes have strong negative reactions, as exemplified in a public outcry after a newspaper offered bonuses to employees in a simulated phishing email [7]. Simulated phishing campaigns can also have more subtle negative effects, such as giving the impression that the IT department is trying to trick employees, of adding an additional burden on employees who are already often under pressure to perform in their job tasks [31] and might even lead to an insider threat through the intentional manipulation of phishing campaigns [15].

In this paper, we explore the factors making a simulated phishing campaign seem (un)acceptable. We conduct a pre-registered between-subjects vignette experiment (N=793) to investigate how various characteristics of a phishing campaign influence its acceptance. In an online experiment, we measured the variation in whether employees gave their prior consent, whether the phishing email promised a financial incentive and what the consequences were for employees when they clicked on the phishing link.

Our results show that prior consent to being involved in a simulated phishing campaign had a positive effect on the acceptance of a phishing campaign, whereas the content of the phishing email, including an incentive, had a negative effect on the acceptance of the campaign. We also found that the various consequences of interacting with the phishing campaign had different effects on the acceptance of the campaign. Varying these dimensions of a simulated campaign did not affect the manipulation probability (to click on the phishing link despite knowledge of the simulated phishing campaign) in a statistically significant way. This means that the intention to interact with a phishing email when someone already assumes that it is a simulated phishing email was not influenced by our measured variables.

Contribution Statement. This paper makes the following contributions:

(1) We conduct a study on the factors that influence the acceptance of simulated phishing campaigns using a vignette experiment, allowing us to make causal statements about factors influencing the acceptance and manipulation probability of simulated phishing campaigns.

(2) We discuss the implications of these results for user-centered security research and cybersecurity practice and highlight how these could inform how organizations conduct anti-phishing training and future research.

2 BACKGROUND

2.1 Phishing and its Consequences

Phishing is a social engineering attack and refers to the process in which sensitive information is elicited from the victim by pretending to be a trusted entity according to an automated pattern [2]. In our digital and connected world, phishing is an important concern in almost every company or government institution [50]. The frequency of phishing attacks is increasing, and their consequences are dire [4, 50]. Attackers predominantly conduct phishing campaigns in emails but also use instant messaging or SMS [24].

Phishing attacks exploit human psychology to encourage potential victims to take certain actions. Several studies argue that phishing emails exploit the general principles of persuasion used in marketing practices, such as Cialdini's persuasive principles of authority, social proof, liking/similarity, commitment/consistency, scarcity, and reciprocation [59, 60]. Among these, the authority and scarcity principles were most prevalent in phishing emails [1]. Attackers use a variety of tactics, such as threatening potential victims and time pressure [30].

Other researchers believe that in addition to Cialdini's principles, it is essential to combine them with tactics used in the field of Social Engineering [19, 51], such as distraction and deception. They argue that the most frequently used tactics in phishing emails are appeals to authority and distraction [20].

A different branch of studies aimed to link the success of phishing attacks to the personal characteristics of the targeted individual. Results indicated that extroversion in the target person might contribute to the success of a phishing attack [3, 33]. Yet, these findings might be questionable due to the absence of a solid psychological foundation [36].

Another set of studies examined the role of cognitive processes in phishing susceptibility. They suggest the goal of phishing attacks is to activate the peripheral processing of information, thereby engaging the target user in lower levels of biased information processing. This bias leans towards subjective reasoning associated with the peripheral route [39].

The consequences of phishing can be devastating and include personal, financial, and societal harm. All it takes is one inattentive user action to open the door for the attacker and enable numerous attacks. An example of real-world consequences related to phishing attacks is the Ukrainian Blackout. In 2015, a spear phishing campaign served as the initial attack vector on the Ukrainian power supply which allowed credentials to be stolen from IT personnel at Ukraine's power companies [13, 35]. The result was the deletion of power plant control systems and a six-hour power outage with about 80,000 people affected [13, 35].

The consequences of effective phishing attacks can extend to financial damage as well, such as when ransomware is used to restrict access to data, followed by demands for payment in exchange for restoring access to the affected data [28]. Victims are often put under time pressure, for example, in that production facilities in an industry plant are no longer functioning, or vital medical equipment in a hospital is no longer working, and thus human lives are at stake [28]. Companies or institutions can also suffer damage to their reputation and the associated trust of customers if a phishing attack is successful [42].

2.2 Phishing Countermeasures

Many companies and authorities attempt to implement effective countermeasures, which include intelligent anomaly detection through machine learning approaches, 2-factor authentication, or sandboxing [41]. But even with the combination of various countermeasures, there is no 100% security, especially in organizations in which employees are expected to interact with actors outside of the organizations. Unfortunately, organizational vulnerability to phishing is difficult to mitigate completely with technical means [49]. There is a race between the defender and attacker: if the filtering rules for phishing attacks improve, the attackers adapt their emails to the target environment. Flores et al. found in a phishing study of 2099 subjects that computer experience has a positive significant correlation with phishing resilience [44]. For this reason, an increasing number of companies and government institutions are focusing on training people in addition to technical countermeasures. This is achieved through training or simulated phishing campaigns.

2.3 Phishing Simulation Campaigns

Phishing simulation campaigns are similar to a real phishing attack, but unlike a real attack, the adversary is a team of offensive forces who are not real attackers. These try to attack the organizational infrastructure via emails tailored to the organization without causing sustainable damage. According to Volkamer et al., this procedure should be precisely defined in advance with the organization's leadership. On one hand, attacking the organizational infrastructure via emails tailored to the organization without causing sustainable damage can be used to show how vulnerable or even protected an organization is, which falls into the penetration testing area [52]. On the other hand, the simulated campaign can also be used to instruct and thus train the employees who have clicked on the link of a simulated phishing email [52]. Simulated campaigns can also be used to formally evaluate the security awareness of an organization's employees [52].

2.4 The Controversy Surrounding Phishing Campaigns

It is unclear whether simulated phishing campaigns lead to the promised outcome of making organizations' employees adopt more secure email behaviors. Researchers have argued that simulated phishing campaigns do not have the intended effects [32, 47, 53]. Simulated phishing campaigns are often costly and the benefits as well as the approach are controversial. In their analysis of hidden costs for phishing simulation campaigns, Brunken et al. showed how extensive and underestimated these costs often are, especially due to the numerous personnel hours involved [10]. Unfortunately, negative consequences cannot always be avoided, as in the case of the US-based newspaper Tribune Publishing and Co. Here, after years of layoffs, staff reductions, and wage cuts, a simulated phishing campaign was conducted, luring with financial bonus payments between $5,000 and $10,000 [7]. Many people were very excited about the false monetary promises, which is why the deception had a very negative impact. As a result, there was public outrage from employees, as well as journalists from other companies, and trust in the leadership and the company in general declined [7]. The question arises as to whether deliberate deception of employees triggers opposing behaviors and leads employees to make manipulative decisions.

In a large-scale study with more than 6,000 employees, Greitzer et al. [23] found that simulated phishing campaigns might even lead to negative outcomes and that employees who have already fallen for a phishing attempt are also more likely to fall for a new phishing attack. Distler conducted an in-situ deception study showing that simulated phishing campaigns can have undesirable consequences, such as shame within a person who interacted with a phishing email, which can lead to inaction after interacting with a phishing email [15]. One explanation here could be a finding by Volkamer et al., which explains that there is a possibility of resignation or loss of motivation on the part of employees if simulations occur too frequently, and even real phishing emails could be mistaken for a simulation, or employees could click on any link as a form of protest [52]. Mihelic et al. showed through a study with 111 subjects that employees lower their attention to a second phishing attack after an attempted one [37]. This behavior could be deliberately provoked to carry out more successful phishing attacks by distracting the employees [37]. Wood also explained the serious consequences of fraud that can be associated with falling for a phishing attack [57]. Psychological factors such as anxiety, depression, shame, disrupted sleep, or even an increased risk of suicide can be a possible negative consequence, which can also apply to simulated phishing campaigns [57]. Therefore, employees may also suffer negative consequences due to a simulated phishing campaign.

The recording of click numbers, i.e., the number of people who clicked on the phishing link, is often used as a performance indicator and is intended to provide a company's management with information about the organization's security awareness. However, click numbers do not capture the circumstances of why people clicked [37]. Also, according to Volkamer et al., the completion of a training or a simulated campaign should not be a mere ticking off of a necessary task and then blaming the employee if they interact with a phishing attack despite having completed the training [52].

2.5 Acceptance of Phishing Simulation Campaigns

Attention must be paid to the acceptance of the company's own employees and stakeholders to avoid negative consequences as in the Tribune case explained above [7]. Employees' acceptance of phishing campaigns describes the approval of a certain implementation. Reed et al. show that positive consequences, when something is added, such as completing training or having a conversation with a supervisor, increase acceptance of the respective consequence more than negative punishments when something is taken away, such as dismissal [43]. The question remains whether the type of consequence can also play an important role in simulated phishing campaigns. Volkamer et al. relate consequences to simulated phishing campaigns and indicate that consequences should always be discussed transparently with employees and not be kept too strict. Otherwise, employees will not report when they have been victims of an attack for fear of consequences [52]. A distinction is made as to whether the organization tells the employee if they have clicked on a phishing link and provides training afterwards, or redirects them to a legitimate website [52]. Jampen et al. also point out the importance of an anti-phishing campaign being adapted to the employees to avoid putting additional pressure on the employees, who might not want to "fail" the training measure. Additional pressure on employees can lead to their health and work performance suffering [29]. This illustrates the importance of employee acceptance for a successful campaign. However, the factors that increase acceptance remain largely unexplored and show that there is still great potential for research in this area.

2.6 Summary

- Phishing is a threat to almost every organization and government institution, and exploits human psychology by appealing to authority and distracting recipients, among other strategies.
- Simulated phishing campaigns are controversial and both phishing and simulated phishing campaigns can lead to a loss of motivation and trust, but also psychological harm such as shame and fear.
- It is essential that employees accept simulated phishing campaigns, as acceptance can influence the effects of simulated phishing campaigns, including effects on employees' view and trust in their employer, and adverse behavioral outcomes (e.g., intentionally boycotting campaigns). We do not currently know which factors influence employee acceptance of simulated anti-phishing campaigns.
- *This paper* investigates the factors that make a simulated phishing campaign seem (un-)acceptable. We conducted a vignette study to address this research gap.

3 RESEARCH OBJECTIVES

We address two main research questions:

RQ1 What factors affect the acceptance of a simulated phishing campaign in an organization?

RQ2 What factors affect the likelihood of the participants to click on the link contained in the phishing email despite knowing that it is a simulated phishing campaign?

Hypotheses. Informed consent is a crucial ethical requirement of most usable privacy and security research [17], where deception studies are rarely conducted [16]. In organizational contexts, the concept of informed consent is somewhat more ambiguous as different legislative and ethical protections are in place than in empirical research. Research emphasizes the significance of psychological contracts for employees' acceptance of an organization's cybersecurity policies [25]. Employees expect organizations to act transparently. Without consent, organizations risk violating this psychological contract, potentially eliciting negative emotional and behavioral reactions from employees [38].

We hypothesize that prior informed and free consent to participating in a simulated phishing campaign would influence employee acceptance of such campaigns.

H1: Obtaining employee consent in advance has a positive effect on the acceptance of the simulated phishing campaign.

The example of a newspaper company conducting a simulated phishing campaign leading to a public outcry [7] provides a negative example of how monetary promises in the phishing email can lead to a severe loss of trust and lasting negative consequences for both the employees and the company if the employees have money problems at the time of the campaign. Here, negative employee sentiment was shown to increase aversion and lack of understanding of the campaign [7]. Hence, we hypothesize that monetary incentives in messages in the context of a phishing campaign might lead to lower acceptance. We formulate the following hypothesis:

H2: The promise of a monetary incentive in phishing email content has a negative effect on the acceptance of the simulated phishing campaign.

The findings of Reed et al. [43] showed that positive consequences (something is added) increase the acceptance of a certain consequence more than negative consequences (something is taken away) like a dismissal. It can therefore be assumed that consequences in which the employee receives something additional, such as an appraisal interview or training, lead to greater acceptance, in contrast to negative consequences in which something is taken away from the employee, such as a dismissal, which trigger lower acceptance. For this reason, we state the hypothesis:

H3: More severe organizational consequences for the employee, resulting from clicking on the phishing link, have a negative effect on the acceptance of the simulated phishing campaign.

Volkamer et al. [52] have shown that employees might intentionally click a phishing link to protest a simulated phishing campaign. For this reason, it can be assumed that the manipulation probability plays an important role in informing employees about the campaign, which is why the following hypothesis is made:

H4: Obtaining employee consent in advance has a negative effect on the employees' intention to click on the phishing link despite knowledge of the simulated phishing campaign.

Employees may intentionally click on a link in a phishing email out of frustration [52]. We hypothesize that promises of money in the phishing message trigger a higher dissonance and that employees feel tricked, which is why the following hypothesis is formulated:

H5: Campaigns in which a monetary incentive is promised have a positive effect on the intention to click on the phishing link despite knowledge of the simulated phishing campaign.

The consequences of simulated phishing campaigns should always be discussed transparently with employees and should not be handled too strictly. Otherwise, employees will not report when they have been the victim of an attack for fear of serious consequences [52]. The extent of the consequence could consequently trigger renewed frustration among employees, which is why they might want to deliberately manipulate the phishing campaign [52]. Thus, knowing the severe consequences of a phishing incident could reinforce the intention to protest. Thus, we hypothesize:

H6: More severe consequences for the employee resulting from clicking on the phishing link have a positive effect on the intention to click on the phishing link despite knowledge of the simulated phishing campaign.

Flores et al. [44] showed that individuals with computer experience exhibit higher phishing resilience. We hypothesize that higher IT affinity leads to generally higher acceptance of phishing campaigns:

H7: Higher affinity for technology correlates with higher acceptance of the simulated phishing campaign.

4 METHODOLOGY

4.1 Research Design

To investigate our research questions, we developed a vignette study to find out what influence the consent obtained at the beginning of a simulated phishing campaign, the consequences after clicking on the link, and the monetary incentive within the phishing message have on the acceptance of the campaign and the manipulation probability. The study was reviewed and approved by the ethics committee of [anonymized]. We conducted an online vignette experiment in July 2023 with a 2 × 4 × 2 (Consent × Consequences × Incentive) between-subjects design. The independent variables *Consent* (Yes vs. No), *Consequences* (No impact vs. Employee interview vs. Training vs. Termination after click on phishing email), and *Monetary Incentive* (Yes vs. No) were measured as independent within-subject factors. We systematically varied the vignettes with respect to the independent variables, resulting in 16 possible scenarios. The scales of *acceptance* and the *manipulation probability* are measured as dependent variables. In addition, we also recorded the participants' affinity for technology. Figure 1 shows the procedure.

Participants first provided informed consent to participate, followed by information about phishing. Participants were then presented with the background information needed and were then randomly assigned to *one* of the 16 vignettes. The between-subjects approach ensured that participants would not guess the exact purpose of the study and could not weigh between different scenarios. After reading through the vignette, participants were asked to assess (1) how likely they were to accept the scenario at hand and (2) how likely the participant would manipulate the scenario despite the knowledge that it was a simulated phishing campaign by their own organization. Last, we asked participants about their prior experience with phishing campaigns, their IT affinity, and demographic variables. We provide the full questionnaire in appendix B.

Pre-tests. To ensure the understandability of the questionnaire, we first asked three experts in user-centered security and human-computer interaction to go through our questionnaire while thinking aloud while filling out the questionnaire. As a result, we refined our question items. We conducted a pre-test with N=35 subjects to detect possible comprehension problems, especially regarding the vignette scenarios. Based on the feedback from the pre-test, we were able to incorporate improvements that should serve to increase the quality of the main study.

4.2 Vignettes

Each participant was exposed to one vignette out of 16 possible vignettes. Figure 2 shows the situation participants were asked to imagine themselves being in. Participants were asked to imagine that they were a caseworker in a company, asked to evaluate the design of a planned, simulated phishing campaign. The vignette first provided information on whether the employer in the scenario would obtain prior consent about the upcoming campaigns from each employee (*Consent: Yes vs. No*). The vignette then explained the content of the planned phishing email. The company's boss asked the employee to open the link and, depending on the scenario, promised a salary increase *(Monetary incentive: Yes vs. No)* if the information contained in the link was presented at the next meeting. Finally, we explained to the subjects the consequences for employees if they fell for the phishing link *(Consequences: No impact vs. Employee interview vs. Training vs. Termination after clicking on a link in a phishing email).*

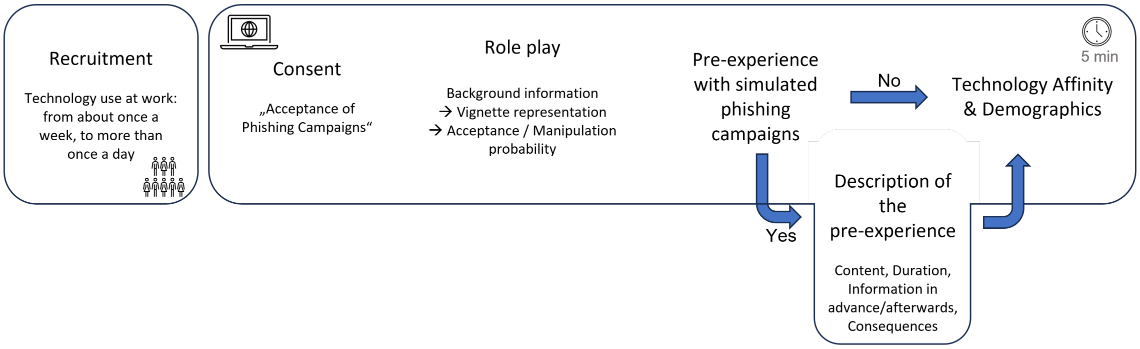
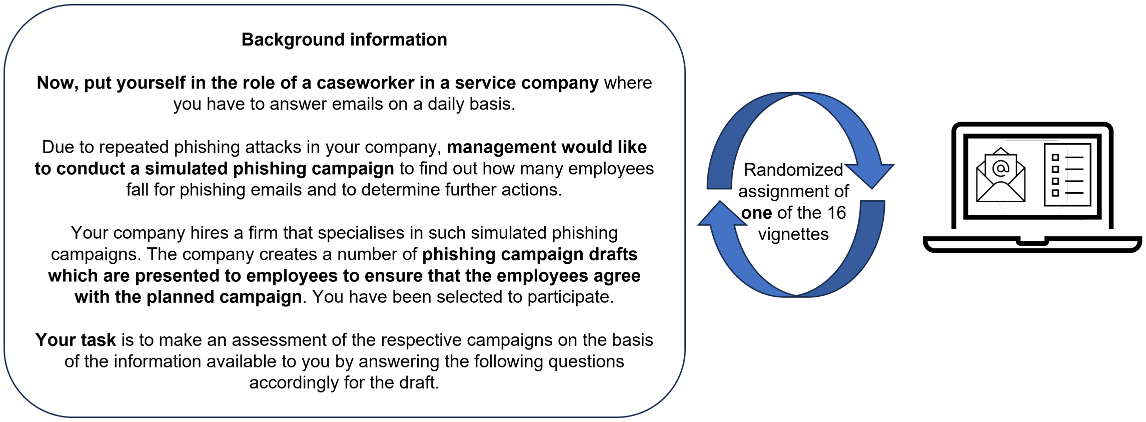

Recruitment
Technology use at work: from about once a week, to more than once a day
Consent
„Acceptance of Phishing Campaigns“
Role play
Background information
→ Vignette representation
→ Acceptance / Manipulation probability
Pre-experience with simulated phishing campaigns
No
Yes
5 min
Technology Affinity & Demographics
Description of the pre-experience
Content, Duration, Information in advance/afterwards, Consequences

Fig. 1. An overview of the study procedure. Participants were recruited on an online platform and used technology at work at least once per week. Participants were asked to situate thesemlves in a roleplay, where they were first given information about phishing, and were then randomly shown one of 16 vignettes describing a simulated phishing campaign scenario. Participants answered questions about how acceptable they found the scenario and how likely the participant would manipulate the scenario despite the knowledge that it was a simulated phishing campaign by their own organization (manipulation probability.


Background information

Now, put yourself in the role of a caseworker in a service company where you have to answer emails on a daily basis.

Due to repeated phishing attacks in your company, **management would like to conduct a simulated phishing campaign** to find out how many employees fall for phishing emails and to determine further actions.

Your company hires a firm that specialises in such simulated phishing campaigns. The company creates a number of **phishing campaign drafts which are presented to employees to ensure that the employees agree with the planned campaign**. You have been selected to participate.

Your task is to make an assessment of the respective campaigns on the basis of the information available to you by answering the following questions accordingly for the draft.

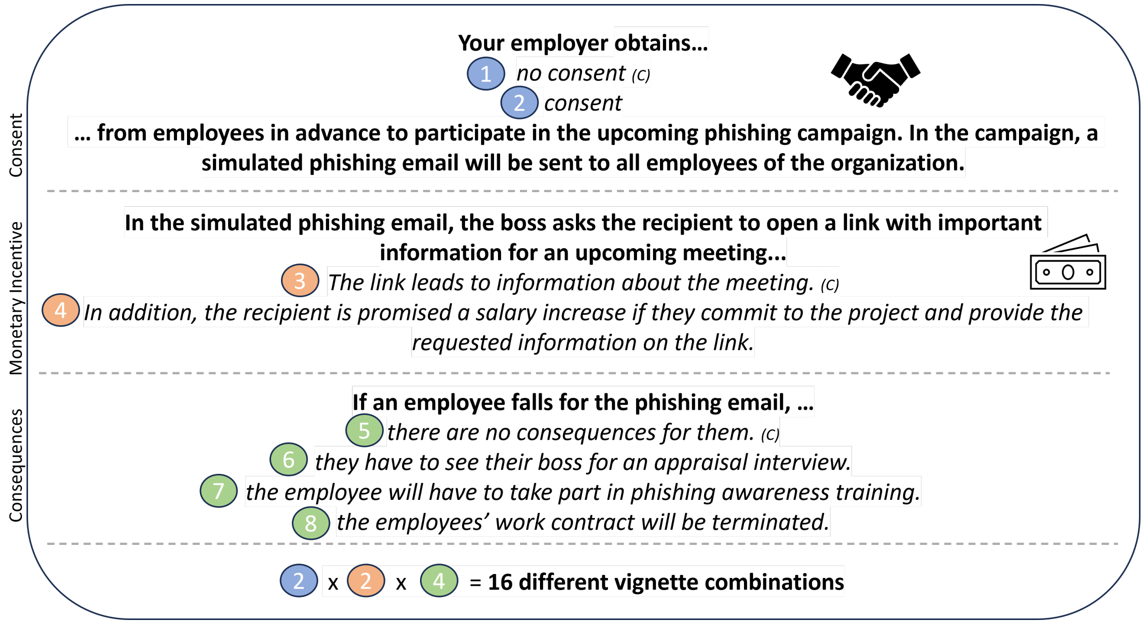
Fig. 2. Background information about the vignettes. This information was shown to all participants, independently of the condition they were assigned to. After this background information, participants were shown one of 16 vignettes.

4.3 Measurements

We asked participants how acceptable they found the design (*acceptance*) and how likely they would be to click on the link despite knowing about the simulated phishing campaign (*manipulation probability*).

4.3.1 Acceptance. Acceptance of the vignette was measured on a 10-point scale (1=Not acceptable at all; 10=Fully acceptable), asking "How acceptable would you find it if this campaign was conducted in this form in your company?".

4.3.2 Manipulation Probability. Manipulation probability was measured with the question "What is the likelihood that you would click on the phishing link if you already realized it was a phishing email from your employer?". Answers were recorded on a 10-point scale from (1) "Very unlikely" to (10) "Very likely." In addition, we asked subjects to justify their decision regarding the likelihood of manipulation within an open response field to better understand the motivations for actively manipulating a simulated phishing campaign.



Your employer obtains…
1 *no consent (C)*
2 *consent*
… from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting…
3 *The link leads to information about the meeting. (C)*
4 *In addition, the recipient is promised a salary increase if they commit to the project and provide the requested information on the link.*

If an employee falls for the phishing email, …
5 *there are no consequences for them. (C)*
6 *they have to see their boss for an appraisal interview.*
7 *the employee will have to take part in phishing awareness training.*
8 *the employees' work contract will be terminated.*

2 x 2 x 4 **= 16 different vignette combinations**

Fig. 3. Representation of the scenario described in the vignettes. The dimensions (consent, monetary incentive, consequences) are separated by a dashed line. The levels within each dimension are numbered. Baseline conditions are highlighted with a (C).

4.3.3 Previous Experience of Phishing Campaigns. After the vignette experiment and independently of the condition a participant was assigned to, we asked the subjects whether they had already been part of a simulated phishing campaign as an employee in a company. This question was a filter question (answer format: yes/no). Participants with prior experience were then asked to describe the campaign in more detail. We chose an open response field and asked participants to provide information on the content, number of phishing emails, duration, and scope of the campaign.

We asked participants with prior experience whether clicking on the phishing link had any consequences, and if so, what these consequences were in an open answer format. In addition, we surveyed whether and how the participants were informed about the campaign in advance and/or afterwards. Participants could choose from the following categories: Not at all (1), Verbally by the supervisor (2), Email (3), Works meeting (4), Training (5), Note during recruitment (6), Other (open response field; 7). Lastly, we recorded on a 6-point scale from 1 (Strongly disagree) to 6 (Strongly agree) how strongly participants agreed that the simulated phishing campaign improved the relationship between them and the employer and whether they rated phishing campaigns as very positive.

4.3.4 IT Affinity. Finally, we recorded the participants' technical affinity using the short version of the Affinity for Technology Interaction Scale (ATI Scale) according to Franke et al. [22].

4.4 Recruitment and Participants

We recruited a sample size of N=793 subjects from Prolific (https://www.prolific.co/) in July 2023. Members of the platform receive a notification when they are eligible for a research study. For our study, we did not use any restrictions regarding gender or education. To participate in the study, participants had to meet the requirement of using technology at work of "about once a week, 2 or 3 times a week, 4 or 6 times a week, about once a day, more than once a day". In addition, participants who had taken part in the pre-test of the study were excluded. Participants had to be UK residents. Our goal was to recruit 800 participants to obtain approximately 50 responses per vignette (50*16 = 800), as 50 responses per vignette are recommended in the literature as a rule of thumb to obtain sufficient statistical power [5].

4.4.1 Data Exclusion. We obtained data from 803 participants who completed the questionnaire in full. In line with our pre-registration, we excluded 10 participants because they reported an English language level of A1 or A2. In the analyses, only data from the study participants who had at least an advanced level of language proficiency at the time of the study would be analyzed (B1 or better). This is to ensure that the participants understand the vignettes, despite the complexity of the subject matter. For this reason, a total sample size of N=793 was used in the analysis.

4.4.2 Description of Sample. Participants were 48.7% female, 50.2% male, 0.6% non-binary, and 0.5% did not indicate their gender. Participants were on average M=41 years old (SD=12.85, Range=18-78). Participants were relatively highly educated, with a large proportion holding bachelor's or master's degrees (details in table T.1 in appendix). Participants showed an average ATI score of technology affinity of M=14.62 (SD=4.59). The Cronbach's alpha is α=.87.

4.5 Experimental Data

Each vignette was shown 49.56 times on average. For the analysis of gender, a t-test was calculated between the dependent variables and the demographic variable. Spearman correlation was calculated for age and Kruskal-Wallis tests were calculated for education to detect differences between groups. We found that males (M=5.76, SD=3.37) reported significantly higher acceptance scale scores than females (M=5.01, SD=3.28; t(782)=-3.20, p<.001, 95% CI [-1.22, -0.29]). With regard to age (p=.50), no significant relationship was found on vignette acceptance, nor were there significant differences with regard to education (p=.35) and acceptance. No significant gender difference was found on the manipulation probability scale (t(782)=-.927, p=.35, 95% CI [-0.15, 0.43]). We found no significant correlations between age (p=.46) and education (p=.31).

We inspected the response behavior across the vignettes. We found a symmetrical data distribution of the responses on the acceptance scale, where the extremes have the highest frequencies and the middle category values have lower frequencies, resulting in a U-shaped response distribution of acceptance (Appendix A.1). All response options were used. The manipulation probability scale shows a right-skewed distribution, with the majority of responses being low values and a very small portion indicating higher values. All response options were used on this scale (Appendix A.2).

The Shaprio-Wilk test showed data not to be normally distributed. Schmidt and Finan's [48] work shows violations of the normal distribution to not noticeably affect the results for large samples (> 10 observations per variable).

4.6 Data Analysis

In separate models, we first estimated the overall effect of our independent variables (consent, monetary incentive, consequences) on the dependent variables' acceptance of the simulated phishing campaign and the manipulation probability. Then, we estimate the effect of the individual characteristics of the independent variables on the dependent variables. If we found a significant effect, we examined between which variable expression the effect is to be found.

In addition, we examined the relationship between individual affinity for technology and the acceptance of simulated phishing campaigns calculating the individual sum score for each person.

We provide the syntax files used for analysis and the data (with potentially harmful metadata removed) as supplementary material.

4.7 Limitations

We could not reproduce every possible scenario or combination possible in reality. Thus, not every possible expression of the independent variables could be represented. However, using our methodological approach, we were able to isolate the effects of our variables and make a statement about the effects of the variables we collected. We acknowledge that the consequence "training" might be perceived differently by different employees. In future work, it would be insightful to further define training measures to understand their relative acceptance.

Our sample consists exclusively of UK residents, which may limit the generalizability of the study results. There may also be cross-cultural differences with regard to the dependent variables of acceptance and manipulation probability.

Lastly, vignettes did not have the same length in their expressions, which is why some vignettes were longer than others. However, each subject was presented with only one vignette, which is why the average duration of the study was 04:54 minutes. For this reason, we assume that no fatigue effects are to be expected during the study.

5 RESULTS

5.1 Bivariate Correlations between Dependent Variables

We performed a correlation analysis of the dependent variables' acceptance and manipulation probability. We found a significant negative correlation (r=-.08, p=.02). This means that higher values in acceptance could tend to be associated with slightly lower values in manipulation probability. However, since the correlation coefficient is close to zero, this indicates that the relationship between these two variables is rather weak. The acceptance rating of the different vignettes was on average M=5.39 (SD=3.34) and the manipulation probability was M=2.12 (SD=2.06).

5.2 Experimental Evidence

5.2.1 Acceptance. We calculated a linear regression between the dependent variable acceptance and the independent variables using a significance level of α=.05. For the evaluation of the hypotheses we refer to the results of the single effects. However, the overall effects are also reported (table T.4 and figure A.3). We found a significant positive effect of obtaining prior consent from employees at the beginning of a phishing campaign on acceptance (r(789)=.28, p<.001). With regard to consequences, a significant negative effect was found on the acceptance (r(789)=.32, p<.001). We found no effect of the monetary incentive on acceptance in the overall effects (r(789)=-.05, p=.07).

To further examine the results, we then calculated the single effects of the levels of the independent variables (see table 1). We found a statistically significant positive effect on acceptance (p<.001). Obtaining consent was found to increase the acceptability rating by almost one scale point (0.90). The single effects of the consequences also showed a significant effect of the variable characteristics, whereby the consequence of an employee interview as a result of clicking on the phishing link caused the acceptance of the campaign to drop by more than one and a half scale points (-1.64). In particular, termination of employment, however, led to a significant drop in the acceptance rating of almost three and a half scale points (-3.37). The two significant effects were significant (p<.001) We found that a monetary incentive caused the acceptance of the phishing campaign to drop by almost half a scale point (-.47). The effect here was statistically significant (p<.05). Figure 4 shows a visual representation of the coefficients.

5.2.2 Manipulation Probability. Overall, participants reported a very low likelihood of clicking on a phishing link if they already realized it was from their employer (see figure A.2). We estimated the overall effect of the independent variables on the dependent variable at a significance level of α=.05. No statistically significant relationship was found

Table 1. Single effects of the independent variables on the acceptance of the simulated phishing campaign. Acceptance was measured on a scale of 1 to 10 (1=Not acceptable at all; 10=Fully acceptable).

Term	Estimate	
Intercept	6.4713***	(0.2520)
Consent	0.9034***	(0.2379)
Incentive	-0.4741*	(0.2075)
Employee interview	-1.6394***	(0.2845)
Training	0.2923	(0.2959)
Termination of contract	-3.3688***	(0.3121)

Standard errors in parentheses
+ p < .10, * p < .05, ** p < .01, *** p < .001

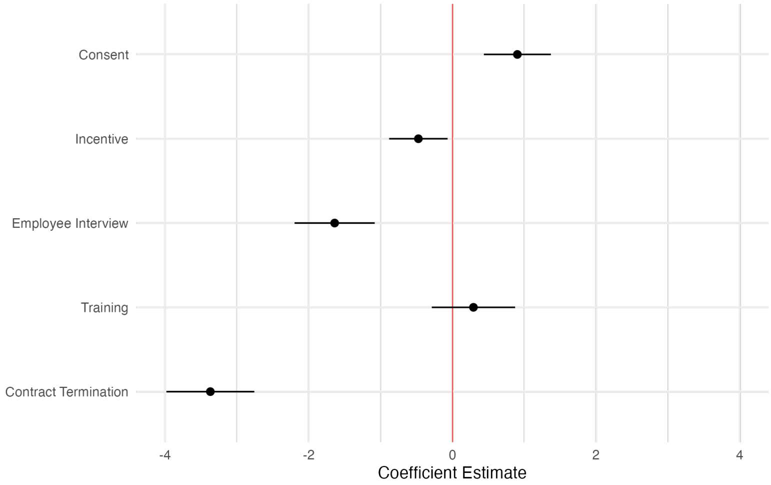


Fig. 4. Coefficient plot single effects of the independent variables on the acceptance of the simulated phishing campaign

between the Consent, Incentive, and Consequences variables and the dependent variable (the overall regression model for manipulation probability can be found in the appendix, table T.5 and figure A.4).

Nevertheless, we then looked at the single effects (see figure 5) of the variable expressions, showing that obtaining consent and a monetary incentive in the context of the phishing email had no statistically significant effects on manipulation probability (*p*>.05).

The answers to the open question, in which participants were asked to explain reasons why they might click on a phishing link if they already know that it is a simulated phishing campaign, indicate that there were three main reasons for intentionally clicking a suspected phishing link from an employer: false trust in the email (*n*=44), protest (*n*=11) and curiosity (*n*=9). Answers such as “The boss has specifically asked me to open it so I would think it is OK” or “I think I’m quite trusting and do as I’m told” showed that participants often have false trust in phishing emails if they assume that it is a legitimate email from their boss. However, protest was also a reason for intentionally clicking on phishing links. For example, participants stated “they shouldn’t be allowed to do it. I don’t think it’s morally right” or “I would still click on the link because I know there is no consequence for me”. Answers such as “Just to read it” or “Just out of curiosity I guess.[...]” show that phishing messages can trigger curiosity in recipients, which leads them to click on the malicious link.

Table 2. Single effects of the independent variables on the manipulation probability. Manipulation probability was measured on a scale of 1 to 10 (1=very unlikely, 10=very likely).

Term	Estimate	
(Intercept)	1.9173	(0.1784)
Consent	0.1116	(0.1684)
Incentive	0.1648	(0.1469)
Employee Interview	0.0714	(0.2014)
Training	0.2832	(0.2095)
Termination of contract	0.0196	(0.2210)

Standard errors in parentheses
+ p < .10, * p < .05, ** p < .01, *** p < .001

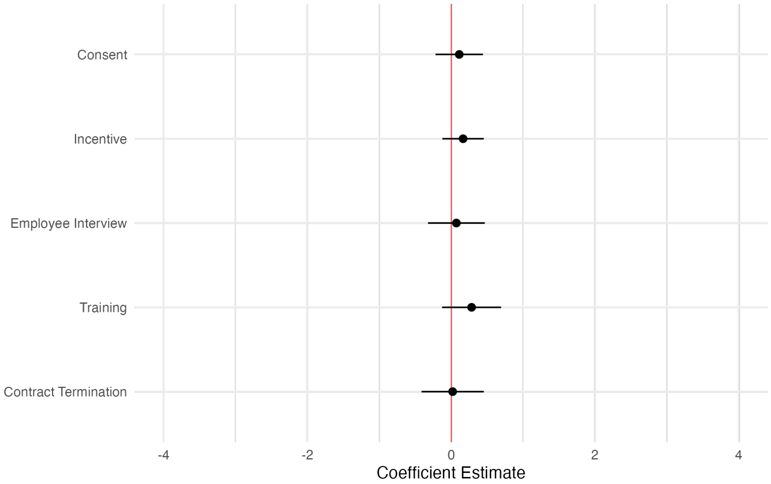


Fig. 5. Coefficient plot of single effects of the independent variables on manipulation probability

5.2.3 ATI and Acceptance. Participants had an average ATI value of *M*=14.62 (*SD*=4.59). To investigate whether technology affinity has an influence on the acceptance of phishing campaigns, we calculated a Pearson correlation due to the violation of the normality assumption. A significant positive correlation was found (*r*(791)=.12, *p*<.001).

This suggests that people with a higher affinity for technology generally rate the acceptance of phishing campaigns higher. Hypothesis 7 can be accepted.

5.3 Prior Experience with Simulated Phishing Campaigns

Of the 793 participants, *n*=179 (23%) indicated prior experience with simulated phishing campaigns and completed the additional questions describing the prior experience. This subsection refers to the answers of this subset of participants. The purpose of this subsection is descriptive and is independent from the experimental treatments. 64% of participants who had previous experience with simulated phishing campaigns were not informed about the campaign in advance. 17% reported being informed by email, 10% as part of training, 7% by the supervisor, and just under 3% each by a work meeting or during the application process. In retrospect, almost 77% said they had been informed about the phishing campaign by email, 10% each in the context of training and/or during a work meeting, 8% verbally by the supervisor, and 5% not at all. A small number of the participants indicated, for example, an information message on the company's intranet site or conversations with the other employees. We found that subjects with prior experience of phishing campaigns rated on average M=3.72 (SD=1.23) that the campaign improved their relationship with the employer. This can be roughly assigned to the response option "Lightly Agree". Also, regarding the question of whether the simulated phishing campaign was rated as very positive, it was shown that participants indicated an average of M=4.58 (SD=1.09), which stands for "Lightly Agree" or "Agree". Overall, 44% of participants with prior experience indicated that falling for the phishing message resulted in consequences for that particular employee. Almost exclusively, participants indicated in the open response field that phishing training was most often the consequence of falling for the phishing campaign.

5.4 Summary of the Results

We summarize the results of this study in table 3.

Table 3. Overview of the results

	Hypothesis	Result	Explanation
1	Obtaining employee consent in advance has a positive effect on the acceptance of the simulated phishing campaign.	Confirmed	Prior consent had a positive effect on the acceptance rating of the phishing campaign.
2	The promise of a monetary incentive in phishing email content has a negative effect on the acceptance of the simulated phishing campaign.	Confirmed	The presence of a monetary incentive had a negative effect on acceptance.
3	More severe organizational consequences for the employee resulting from clicking on the phishing link have a negative effect on the acceptance of the simulated phishing campaign.	Partially confirmed	Training had a slight positive, yet statistically non-significant effect on acceptance. An employee interview or termination of the employment relationship had a statistically significant negative effect on acceptance.
4	Obtaining employee consent in advance has a negative effect on the employees' intention to click on the phishing link despite knowledge of the simulated phishing campaign.	Not confirmed	No statistically significant effect of prior consent on manipulation probability could be found.
5	Campaigns in which a monetary incentive is promised have a positive effect on the intention to click on the phishing link despite knowledge of the simulated phishing campaign.	Not confirmed	No statistically significant effect of monetary incentive on manipulation probability.
6	More severe consequences for the employee resulting from clicking on the phishing link have a positive effect on the intention to click on the phishing link despite knowledge of the simulated phishing campaign.	Not confirmed	No statistically significant effect of stronger consequences on manipulation probability could be found.
7	Higher affinity for technology correlates with higher acceptance of the simulated phishing campaign.	Confirmed	People with a higher IT affinity rated the acceptance of phishing campaigns higher.

6 DISCUSSION

6.1 Acceptance

Consent and simulated phishing campaigns. Consent and simulated phishing campaigns are a debated topic. In our study, consent positively influenced the acceptance rating, but in practice, simulated phishing campaigns typically involve deception [52]. For example, some organizations never disclose the fact that a simulated campaign has been conducted and simply redirect the victim to a legitimate website. Others inform the victim once fallen for a simulated phish [52].

Securing consent before initiating simulated phishing training can be understood through the lens of the "psychological contract". The psychological contract outlines the implicit expectations between employees and employers regarding mutual responsibilities [45]. Prior research emphasizes the significance of psychological contracts for employees' acceptance of an organization's cybersecurity policies [25]. Studies also indicate that employees perceive justice and fairness as core components of these psychological contracts [26]. Essentially, employees expect organizations to act transparently and declare their intentions openly. Without clear consent for simulated phishing emails, organizations risk violating this psychological contract. Such violations can elicit negative emotional and behavioral reactions from employees [38], potentially diminishing their commitment to the organization's security measures [34].

Reactance theory offers an alternative perspective on the importance of consent in simulated phishing campaign acceptance. Reactance is described as a negative emotional response triggered by perceived threats or limitations on an individual's behavioral freedom [9]. Within organizations, this type of response frequently emerges in relation to security measures that aim to regulate employee behavior [58]. When an organization initiates a simulated phishing campaign without obtaining employee consent, it can be perceived as a restriction on their freedom to choose to participate. This might provoke negative reactions, such as employees deliberately clicking on phishing links, which counters the organization's objectives.

Informed consent is considered an important ethical safeguard in most empirical studies in usable privacy and security [17], but the amount of information that should be provided to participants in research to qualify as informed consent is often unclear [8]. Providing lengthy documents is not necessarily informative for research participants, or employees. Prospective research participants often do not understand the information disclosed to them in the informed consent process [21], and similar issues could arise with employees. More investigation is needed to understand how employees might best be informed about simulated phishing campaigns in ways that both respect their time and provide all necessary information. Simulated phishing campaigns generate personal, and potentially sensitive, information about employees. An informed consent procedure should, at the very least, clarify who would gain access to information about employees' behavior, how long this information will be stored, how it will be secured, and how consent can be revoked (additional considerations can be found in [52]). A useful resource when defining a meaningfully informed consent procedure is the GDPR consent requirements [56], which mention for example that consent should be informed and freely given. As an example, following this standard, employees who do not consent to participate in a simulated phishing campaign should be given other options to learn about phishing countermeasures. The acceptance rating of the various simulated phishing campaigns was generally in the medium range. This can be interpreted to mean that the participants tended to give a neutral acceptance rating for the various phishing campaign scenarios, which were rated neither particularly positively nor particularly negatively. It could be useful to promote knowledge about phishing campaigns among employees in order to simultaneously counteract doubts or negative emotions in this regard and increase acceptance. Any security measures could also be conceptualized and refined in co-design sessions with employees, taking into account their thoughts and experiences in their daily work life.

False promises of monetary incentives. We found that the content of the email containing the promise of a monetary incentive had a small yet statistically significant negative effect. This finding is in line with the previously mentioned example of the journal conducting a simulated phishing campaign [7]. In a real-life phishing campaign, the effect of a promised incentive will depend on the organizational context, and it is important to consider that other pretexts may also have a negative effect on acceptance. Sensitive topics might include, in addition to financial incentives, vacation days, sick leave, and organizational restructuring.

Consequences of interacting with a phishing email. Depending on the consequences described in the vignette scenario, acceptance ratings differed (see figure 4). While both contract termination (in line with [43]) and an employee interview had a negative effect, training as a consequence had a non-statistically significant negative effect. We hypothesize that the effect of training on acceptance will depend on a variety of factors, including the duration of the training measure, whether the training is perceived as "embarrassing" (e.g., if supervisors are informed) or as helpful.

6.2 Manipulation Probability

Previous work has mentioned the possibility of employees manipulating intentional clicking as a protest because they feel it is unreasonable for their organization to "trick" them in this way, or out of curiosity [52]. In our study, most participants indicated that they would not knowingly click on a simulated phishing email from their employer and it is noteworthy that none of the vignette factors showed a statistically significant effect on manipulation probability. In the open-ended answers, we did find some indication of clicking out of curiosity or because the participant would not expect any real consequences from clicking. There are multiple possible follow-up hypotheses. The intention to manipulate a simulated phishing campaign might not be very common in general, which explains why we rarely observed it in our sample. It is also possible that the intention to manipulate a simulated phishing campaign is bound to the real-life context of an organizational simulated phishing campaign, and can not easily be replicated using a vignette scenario. For instance, [14] point to the tensions that arise in organizational contexts when time constraints, resource constraints, cognitive constraints, and incomplete information collide with contradictory approaches to secure behaviors in organizations, which can lead to employees making "good enough" decisions. Indeed, time, resource and time constraints cannot easily be replicated outside a realistic work context, and it is possible that manipulation probability is a phenomenon that appears only in the presence of such real-world tensions. There might also be a social desirability effect discouraging research participants from reporting what they may perceive as anti-social behavior in an attempt to present themselves in a positive light [40].

6.3 IT Affinity

Finally, the study focused on whether a higher IT affinity leads to a higher acceptance of phishing campaigns. Similarly, Flores et al. [44] found that individuals with computer experience have a higher phishing resilience.

7 RECOMMENDATIONS

We make some practical recommendations for future simulated phishing campaigns based on our findings. Note that our study does not investigate whether simulated phishing campaigns actually lead to behavioral outcomes that are beneficial for the security of a company. Our recommendations relate to increasing the acceptance of a simulated phishing campaign, thereby potentially counteracting possible negative effects such as loss of trust in the employer or the cybersecurity professionals within the organization.

Obtain consent from participants before including them in simulated phishing training. Our study points to a positive effect of obtaining employee consent in advance of simulated phishing campaigns on acceptance. There is a trade-off between obtaining consent and potentially influencing employees' future behavior since they have been warned. However, the objective of any security measure must be to keep up long-term engagement with security measures, as well as trust in the security professionals of a company. Thus, it seems worthwhile to conduct simulated phishing campaigns after obtaining employee consent and to carefully measure the effects of such prior consent. Employees who do not provide informed consent should be given the opportunity to participate in other types of security training. In addition, the knowledge of being part of a simulated phishing campaign is likely to influence behavior more in the short term.

Clarify the consequences of insecure behaviors in advance of a simulated phishing campaign. Consequences (positive and negative) should be defined in collaboration with employees of an organization. We found that the consequences of a phishing campaign influence its acceptance. Combined with prior informed consent, we recommend consequences of simulated anti-phishing campaigns be made clear. Organizations should clarify what the intentions of the simulated phishing campaign are, which consequences can arise for employees (positive or negative), and exactly how their data is used (e.g., who can access it, is it used to evaluate performance). We found that employee interviews lead to a lower acceptance of the simulated phishing campaign, which might be relevant for smaller organizations in which such a measure might be more realistic. There is also no evidence that such an employee interview would have a positive effect on phishing behavior.

Organizations should carefully consider whether certain pretexts in a simulated phishing email are acceptable for their employees. Promising an incentive in the email had a negative effect on the acceptance of the campaign. While attackers might take certain means to trick victims, organizations should focus on up-keeping long-term engagement with security, rather than tricking employees in the same manner.

Adapt information about simulated phishing campaigns depending on the IT affinity of the employees who will be targeted. We found that IT affinity and acceptance were positively correlated. It is likely that people in certain services of an organization have higher IT affinity (e.g., more technical roles). If employees with a higher IT affinity belong to specific groups (IT specialists) or subcultures within the organization, these groups could serve as endorsers of simulated phishing campaigns. They can then convey the importance of these measures to other employee groups.

8 FUTURE RESEARCH

Future work should investigate the real-life acceptance of employees who have been included in simulated phishing campaigns in their organizations. It would be especially insightful to interview employees who did not agree with the simulated phishing campaign, to identify possible improvements. In addition, it would be relevant to understand how employees think these campaigns affected their behavior. Behavior change in organizational contexts is complex and multi-faceted. The recent framework on behavior change for security behavior in organizations could be useful [46].

Future research should go into more detail regarding the characteristics of the simulated phishing campaign. For instance, while we varied the presence of a promised incentive in the email content, future work could investigate the effects different types of incentives have on the acceptance of the campaign. Similarly, the description of training-related consequences could be varied to understand what makes a training measure more or less acceptable.

9 CONCLUSION

Our results demonstrate the effects of varying certain factors (consent, monetary incentive, consequences) when designing simulated phishing campaigns. We found that the factors examined can have different influences on employee acceptance. Note, however, that this study does not investigate or take a stance on the effectiveness of such campaigns to increase organizational security, which has been questioned by multiple studies. We hope that future work will investigate both the ways in which anti-phishing training (simulated or other) can be made more effective, as well as accepted by employees. Organizations depend on the long-term collaboration and motivation of their employees to stay safe from outside threats, and any security measure should be evaluated in terms of both behavioral effects and how acceptable the measure is perceived by employees. We hope to see more research that investigates employee engagement, motivation and acceptance of security measures.

REFERENCES

[1] Nurul Akbar. 2014. *Analysing persuasion principles in phishing emails.* Master's thesis. University of Twente.

[2] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. 2021. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science* 3 (2021), 563060.

[3] Ibrahim Alseadoon, MFI Othman, and Taizan Chan. 2015. What is the influence of users' characteristics on their ability to detect phishing emails?. In *Advanced Computer and Communication Engineering Technology: Proceedings of the 1st International Conference on Communication and Computer Engineering*. Springer, 949–962.

[4] TAPWG APWG. 2022. Phishing activity trends reports.

[5] Katrin Auspurg and Thomas Hinz. 2015. Multifactorial experiments in surveys. In *Experimente in den Sozialwissenschaften*. Nomos Verlagsgesellschaft mbH & Co. KG, 294–320.

[6] Fabian Lucas Ballreich, Melanie Volkamer, Dirk Müllmann, Benjamin Maximilian Berens, Elena Marie Häußler, and Karen V. Renaud. 2023. Encouraging Organisational Information Security Incident Reporting. In *Proceedings of the 2023 European Symposium on Usable Security* (<conf-loc>, <city>Copenhagen</city>, <country>Denmark</country>, </conf-loc>) *(EuroUSEC '23)*. Association for Computing Machinery, New York, NY, USA, 224–236. https://doi.org/10.1145/3617072.3617098

[7] Jeremy Barr. 2020. The company email promised bonuses. It was a hoax — and Tribune Publishing employees are furious. https://www.washingtonpost.com/media/2020/09/23/tribune-bonus-email-phishing-hoax/

[8] Lydia A Bazzano, Jaquail Durant, and Paula Rhode Brantley. 2021. A modern history of informed consent and the role of key information. *Ochsner Journal* 21, 1 (2021), 81–85.

[9] Sharon S Brehm and Jack W Brehm. 2013. *Psychological reactance: A theory of freedom and control.* Academic Press.

[10] Lina Brunken, Annalina Buckmann, Jonas Hielscher, and M. Angela Sasse. 2023. "To Do This Properly, You Need More Resources": The Hidden Costs of Introducing Simulated Phishing Campaigns. In *32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, Anaheim, CA, 4105–4122. https://www.usenix.org/conference/usenixsecurity23/presentation/brunken

[11] Deanna D Caputo, Shari Lawrence Pfleeger, Jesse D Freeman, and M Eric Johnson. 2013. Going spear phishing: Exploring embedded training and awareness. *IEEE security & privacy* 12, 1 (2013), 28–38.

[12] Kang Leng Chiew, Kelvin Sheng Chek Yong, and Choon Lin Tan. 2018. A survey of phishing attacks: Their types, vectors and technical approaches. *Expert Systems with Applications* 106 (2018), 1–20. https://doi.org/10.1016/j.eswa.2018.03.050

[13] Michał Choraś, Rafał Kozik, Adam Flizikowski, Witold Hołubowicz, and Rafał Renk. 2016. Cyber threats impacting critical infrastructures. *Managing the complexity of critical infrastructures: A modelling and simulation approach* (2016), 139–161.

[14] Albesë Demjaha, Simon Parkin, David Pym, Thomas Groß, and Luca Viganò. 2022. The Boundedly Rational Employee: Security Economics for Behaviour Intervention Support in Organizations1. *J. Comput. Secur.* 30, 3 (jan 2022), 435–464. https://doi.org/10.3233/JCS-210046

[15] Verena Distler. 2023. The Influence of Context on Response to Spear-Phishing Attacks: an In-Situ Deception Study. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–18.

[16] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig. 2021. A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. *ACM Trans. Comput.-Hum. Interact.* 28, 6, Article 43 (dec 2021), 50 pages. https://doi.org/10.1145/3469845

[17] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Vincent Koenig, and Lorrie Faith Cranor. 2023. *Empirical Research Methods in Usable Privacy and Security.* Springer International Publishing, Cham, 29–53. https://doi.org/10.1007/978-3-031-28643-8_3

[18] Ronald C Dodge Jr, Curtis Carver, and Aaron J Ferguson. 2007. Phishing for user security awareness. *computers & security* 26, 1 (2007), 73–80.

[19] Ana Ferreira, Lynne Coventry, and Gabriele Lenzini. 2015. Principles of persuasion in social engineering and their use in phishing. In *Human Aspects of Information Security, Privacy, and Trust: Third International Conference, HAS 2015, Held as Part of HCI International 2015, Los Angeles, CA, USA, August 2-7, 2015. Proceedings 3*. Springer, 36–47.

[20] Ana Ferreira and Soraia Teles. 2019. Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies* 125 (2019), 19–31.

[21] J. Flory and E. Emmanuel. [n. d.]. Interventions to improve research participants' understanding in informed consent for research. A systematic review. 139, 2 ([n. d.]), 399. https://doi.org/10.1016/j.ajo.2004.12.040

[22] Thomas Franke, Christiane Attig, and Daniel Wessel. 2019. A personal resource for technology interaction: development and validation of the affinity for technology interaction (ATI) scale. *International Journal of Human–Computer Interaction* 35, 6 (2019), 456–467.

[23] Frank L Greitzer, Wanru Li, Kathryn B Laskey, James Lee, and Justin Purl. 2021. Experimental investigation of technical and human factors related to phishing susceptibility. *ACM Transactions on Social Computing* 4, 2 (2021), 1–48.

[24] Payas Gupta, Bharat Srinivasan, Vijay Balasubramaniyan, and Mustaque Ahamad. 2015. Phoneypot: Data-driven understanding of telephony threats.. In *NDSS*, Vol. 107. 108.

[25] JinYoung Han, Yoo Jung Kim, and Hyungjin Kim. 2017. An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security* 66 (2017), 52–65.

[26] Peter Herriot, WEG Manning, and Jennifer M Kidd. 1997. The content of the psychological contract. *British Journal of management* 8, 2 (1997), 151–162.

[27] Gert J Homsma, Cathy Van Dyck, Dick De Gilder, Paul L Koopman, and Tom Elfring. 2009. Learning from error: The influence of error incident characteristics. *Journal of Business Research* 62, 1 (2009), 115–122.

[28] Margaret House. 2021. Attributing Deaths to Ransomware Attacks on Hospitals and Medical Care Facilities. https://www.cyber.forum.yale.edu/blog/2021/7/20/attributing-deaths-to-ransomware-attacks-on-hospitals-and-medical-care-facilities

[29] Daniel Jampen, Gürkan Gür, Thomas Sutter, and Bernhard Tellenbach. 2020. Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences* 10, 1 (2020), 1–41.

[30] Mousa Jari. 2022. An Overview of Phishing Victimization: Human Factors, Training and the Role of Emotions. *arXiv preprint arXiv:2209.11197* (2022).

[31] Iacovos Kirlappos, Simon Parkin, and M Angela Sasse. 2014. Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security.

[32] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. 2022. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 842–859.

[33] Patrick Lawson, Olga Zielinska, Carl Pearson, and Christopher B Mayhorn. 2017. Interaction of personality and persuasion tactics in email phishing attacks. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 61. SAGE Publications Sage CA: Los Angeles, CA, 1331–1333.

[34] Daeun Lee, Harjinder Singh Lallie, and Nadine Michaelides. 2023. The impact of an employee's psychological contract breach on compliance with information security policies: intrinsic and extrinsic motivation. *Cognition, Technology & Work* (2023), 1–17.

[35] Gaoqi Liang, Steven R Weller, Junhua Zhao, Fengji Luo, and Zhao Yang Dong. 2016. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE transactions on power systems* 32, 4 (2016), 3317–3318.

[36] Pablo López-Aguilar, Constantinos Patsakis, and Agusti Solanas. 2022. The Role of Extraversion in Phishing Victimisation: A Systematic Literature Review. In *2022 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 1–10.

[37] Anže Mihelič, Matej Jevšček, Simon Vrhovec, and Igor Bernik. 2019. Testing the human backdoor: Organizational response to a phishing campaign. *Journal of Universal Computer Science* 25, 11 (2019), 1458–1477.

[38] Elizabeth Wolfe Morrison and Sandra L Robinson. 1997. When employees feel betrayed: A model of how psychological contract violation develops. *Academy of management Review* 22, 1 (1997), 226–256.

[39] Paula MW Musuva, Katherine W Getao, and Christopher K Chepken. 2019. A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Computers in Human Behavior* 94 (2019), 154–175.

[40] Delroy L. Paulhus. [n. d.]. Socially Desirable Responding on Self-Reports. In *Encyclopedia of Personality and Individual Differences*, Virgil Zeigler-Hill and Todd K. Shackelford (Eds.). Springer International Publishing, 1–5. https://doi.org/10.1007/978-3-319-28099-8_1349-1

[41] Swapan Purkait. 2012. Phishing counter measures and their effectiveness–literature review. *Information Management & Computer Security* 20, 5 (2012), 382–420.

[42] James W. Ragucci and Stefan A. Robila. 2006. Societal Aspects of Phishing. In *2006 IEEE International Symposium on Technology and Society*. 1–5. https://doi.org/10.1109/ISTAS.2006.4375893

[43] Florence D DiGennaro Reed and Benjamin J Lovett. 2007. Views on the efficacy and ethics of punishment: Results from a national survey. *International Journal of Behavioral Consultation and Therapy* 4, 1 (2007), 61.

[44] Waldo Rocha Flores, Hannes Holm, Marcus Nohlberg, and Mathias Ekstedt. 2015. Investigating personal determinants of phishing and the effect of national culture. *Information & Computer Security* 23, 2 (2015), 178–199.

[45] Denise M Rousseau. 1989. Psychological and implied contracts in organizations. *Employee responsibilities and rights journal* 2 (1989), 121–139.

[46] M. Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. [n. d.]. Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours. In *Computer Security. ESORICS 2022 International Workshops*, Sokratis Katsikas, Frédéric Cuppens, Christos Kalloniatis, John Mylopoulos, Frank Pallas, Jörg Pohle, M. Angela Sasse, Habtamu Abie, Silvio Ranise, Luca Verderame, Enrico Cambiaso, Jorge Maestre Vidal, Marco Antonio Sotelo Monge, Massimiliano Albanese, Basel Katt, Sandeep Pirbhulal, and Ankur Shukla (Eds.). Vol. 13785. Springer International Publishing, 248–265. https://doi.org/10.1007/978-3-031-25460-4_14 Series Title: Lecture Notes in Computer Science.

[47] M. Angela Sasse, Jonas Hielscher, and Marco Gutfleisch. 2022. Human-Centred Security: Unfug Informationssicherheits-Sensibilisierung. *kma - Klinik Management aktuell* 27, 04 (Aug. 2022), 44–46. 44.

[48] Amand F Schmidt and Chris Finan. 2018. Linear regression and the normality assumption. *Journal of clinical epidemiology* 98 (2018), 146–151.

[49] Antesar M. Shabut, K T Lwin, and M A Hossain. 2016. Cyber attacks, countermeasures, and protection schemes — A state of the art survey. In *2016 10th International Conference on Software, Knowledge, Information Management Applications (SKIMA)*. 37–44. https://doi.org/10.1109/SKIMA.2016.7916194

[50] Pawankumar Sharma, Bibhu Dash, and Meraj Farheen Ansari. 2022. Anti-phishing techniques–a review of Cyber Defense Mechanisms. *International Journal of Advanced Research in Computer and Communication Engineering ISO* 3297 (2022), 2007.

[51] Tatyana Stojnic, Dinusha Vatsalan, and Nalin AG Arachchilage. 2021. Phishing email strategies: understanding cybercriminals' strategies of crafting phishing emails. *Security and privacy* 4, 5 (2021), e165.

[52] Melanie Volkamer, Martina Angela Sasse, and Franziska Boehm. 2020. Analysing simulated phishing campaigns for staff. In *Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, September 17–18, 2020, Revised Selected Papers 25*. Springer, 312–328.

[53] Melanie Volkamer, Martina A. Sasse, and Franziska Boehm. 2020. Phishing-Kampagnen zur Steigerung der Mitarbeiter-Awareness: Analyse aus verschiedenen Blickwinkeln – Security, Recht und Faktor Mensch. *Datenschutz und Datensicherheit - DuD* 44, 8 (Aug. 2020), 518–521. https://doi.org/10.1007/s11623-020-1317-x

[54] Rick Wash. [n. d.]. How Experts Detect Phishing Scam Emails. 4 ([n. d.]). Issue CSCW2. https://doi.org/10.1145/3415231 Place: New York, NY, USA Publisher: Association for Computing Machinery.

[55] Carly Wilson and David Argles. 2011. The fight against phishing: Technology, the end user and legislation. 501–504. https://doi.org/10.1109/i-Society18435.2011.5978553

[56] Ben Wolford. [n. d.]. *What are the GDPR consent requirements?* https://gdpr.eu/gdpr-consent-requirements/ Section: News & Updates.

[57] Stacy Wood. 2021. How Does Fraud Impact Emotional Well-Being? *Psychology Today* (2021). https://www.psychologytoday.com/us/blog/the-fraud-crisis/202101/how-does-fraud-impact-emotional-well-being

[58] Allison Brown Yost, Tara S Behrend, Garett Howardson, Jessica Badger Darrow, and Jaclyn M Jensen. 2019. Reactance to electronic surveillance: a test of antecedents and outcomes. *Journal of Business and Psychology* 34 (2019), 71–86.

[59] Olga Zielinska, Allaire Welk, Christopher B Mayhorn, and Emerson Murphy-Hill. 2016. The persuasive phish: Examining the social psychological principles hidden in phishing emails. In *Proceedings of the Symposium and Bootcamp on the Science of Security*. 126–126.

[60] Olga A Zielinska, Allaire K Welk, Christopher B Mayhorn, and Emerson Murphy-Hill. 2016. A temporal analysis of persuasion principles in phishing emails. In *Proceedings of the human factors and ergonomics society annual meeting*, Vol. 60. SAGE Publications Sage CA: Los Angeles, CA, 765–769.

A DATASET AND ANALYSIS SYNTAX

We provide the full dataset and analysis syntax as supplemental material.

B FULL QUESTIONNAIRE

PAGE 01

1. Dear participant, thank you for your interest in our study! :-)

We invite you to participate in our study “Acceptance of Phishing Campaigns”. This study is conducted by our University.
In this study, we present a simulated phishing campaign and ask you questions about it as well as about your personal experiences with phishing campaigns. If you agree to participate in this study, you will be asked to complete an online survey. The survey will take approximately 5 minutes to complete. There is no right or wrong when answering the questions in the questionnaire. Your participation in this study is voluntary and you may stop participating at any time without giving a reason.

Data protection notice: Your data will be collected, processed and used for the purpose of conducting and scientifically evaluating the aforementioned research project. The data of this survey will be treated strictly confidential. Linking the survey contents with your person is not possible at any time. The survey contents are collected and processed by the Institute for Application Security (Faculty of Computer Science) based on your consent (6 para. 1 sentence 1 lit. a EU-GDPR). After completion of the questionnaire, the anonymous contents will be further processed. The collected anonymous data can be used for scientific publications.

Recall option: We will remove your Prolific ID to analyse the data. After this point, it is not possible to revoke your consent. If you have any questions about the study, you may contact us. For questions about your rights as a study subject, you can contact the head of the study. By clicking “Yes, I agree” below, you acknowledge that you are at least 18 years old, have read and understood this informed consent form, and agree to participate in this study.

○ Yes, I agree.

○ No, I don’t agree

PAGE 02

2. Please enter your unique Prolific ID:

PAGE 03

Read the following information carefully:

In the following, we present a simulated phishing campaign. In a **phishing attack**, the attacker attempts to obtain sensitive data from the victim, such as login data for user accounts. Fake e-mails or links pointing to fake websites are often used for this purpose. Phishing attacks are taking on an ever-increasing role in today's world and are a major threat to the victim or the company behind them. For this reason, companies run **simulated phishing campaigns** by sending simulated phishing emails to employees in order to assess phishing resistance and train employees.

Please position yourself in the situation as much as possible before answering the questions.

PAGE 04

Background information

Now, put yourself in the role of a caseworker in a service company where you have to answer emails on a daily basis.

Due to repeated phishing attacks in your company, **management would like to conduct a simulated phishing campaign** to find out how many employees fall for phishing emails and to determine further actions.

Your company hires a firm that specialises in such simulated phishing campaigns. The company creates a number of **phishing campaign drafts which are presented to employees to ensure that the employees agree with the planned campaign**. You have been selected to participate.

Your task is to make an assessment of the respective campaigns on the basis of the information available to you by answering the following questions accordingly for the draft.

PAGE 05

Vignette 01

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. In addition, the recipient is promised a salary increase if they commit to the project and provide the requested information on the link.

If an employee falls for the phishing email, there are no consequences for them.

3. How acceptable would you find it if this campaign was conducted in this form in your company?

Not acceptable at all									Fully acceptable
1	2	3	4	5	6	7	8	9	10

4. What is the likelihood that you would click on the phishing link if you already realized it was a phishing email from your employer?

Very unlikely									Very likely
1	2	3	4	5	6	7	8	9	10

5. Why did you make this decision? Please give reasons for your previous answer from question 4.

Vignette 02

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. The link leads to information about the meeting.

If an employee falls for the phishing email, there are no consequences for them.

Vignette 03

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. In addition, the recipient is promised a salary increase if they commit to the project and provide the requested information on the link.

If an employee falls for the phishing email, they have to see their boss for an appraisal interview.

Vignette 04

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. The link leads to information about the meeting.

If an employee falls for the phishing email, they have to see their boss for an appraisal interview.

Vignette 05

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. In addition, the recipient is promised a salary increase if they commit to the project and provide the requested information on the link.

If an employee falls for the phishing email, the employee will have to take part in phishing awareness training.

Vignette 06

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. The link leads to information about the meeting.

If an employee falls for the phishing email, the employee will have to take part in phishing awareness training.

Vignette 07

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. In addition, the recipient is promised a salary increase if they commit to the project and provide the requested information on the link.

If an employee falls for the phishing email, the employees' work contract will be terminated.

Vignette 08

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. The link leads to information about the meeting.

If an employee falls for the phishing email, the employees' work contract will be terminated.

Vignette 09

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains no consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. In addition, the recipient is promised a salary increase if they commit to the project and provide the requested information on the link.

If an employee falls for the phishing email, there are no consequences for them.

Vignette 10

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains no consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. The link leads to information about the meeting.

If an employee falls for the phishing email, there are no consequences for them.

Vignette 11

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains no consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. In addition, the recipient is promised a salary increase if they commit to the project and provide the requested information on the link.

If an employee falls for the phishing email, they have to see their boss for an appraisal interview.

Vignette 12

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains no consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. The link leads to information about the meeting.

If an employee falls for the phishing email, they have to see their boss for an appraisal interview.

Vignette 13

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains no consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. In addition, the recipient is promised a salary increase if they commit to the project and provide the requested information on the link.

If an employee falls for the phishing email, the employee will have to take part in phishing awareness training.

Vignette 14

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains no consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. The link leads to information about the meeting.

If an employee falls for the phishing email, the employee will have to take part in phishing awareness training.

Vignette 15

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains no consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. In addition, the recipient is promised a salary increase if they commit to the project and provide the requested information on the link.

If an employee falls for the phishing email, the employees' work contract will be terminated.

Vignette 16

Please put yourself in the following situation and evaluate the following draft of the simulated phishing campaign:

Your employer obtains no consent from employees in advance to participate in the upcoming phishing campaign. In the campaign, a simulated phishing email will be sent to all employees of the organization.

In the simulated phishing email, the boss asks the recipient to open a link with important information for an upcoming meeting. The link leads to information about the meeting.

If an employee falls for the phishing email, the employees' work contract will be terminated.

PAGE 06

6. Have you ever been part of a simulated phishing campaign by your employer, to your knowledge?

○ Yes

○ No

PAGE 07

7. What exactly was the content of the mail? How many phishing emails have you received from your company as part of the phishing campaign?

You are welcome to give details of the duration, scope, content, etc. in bullet points.

8. Were there any consequences for the employees who fell for the simulated phishing message and, for example, clicked on the link?

○ Yes, for example:
○ No

9. How were you informed about the phishing campaign in advance?

○ Not at all
○ Verbally by the supervisor
○ E-mail
○ Works meeting
○ Training
○ Note during recruitment
○ Other:

10. How were you informed about the phishing campaign after the fact?

○ Not at all
○ Verbally by the supervisor
○ E-mail
○ Works meeting
○ Training
○ Note during recruitment
○ Other:

11. How strongly do you agree with the following statements?

	Strongly disagree	Disagree	Lightly Disagree	Lightly Agree	Agree	Strongly agree
Running the simulated phishing campaign improved my relationship with my employer.	O	O	O	O	O	O
I find the simulated phishing campaigns very positive.	O	O	O	O	O	O

PAGE 08

12. In the following questionnaire, we will ask you about your interaction with technical systems. The term “technical systems” refers to apps and other software applications, as well as entire digital devices (e.g., mobile phone, computer, TV, car navigation).

	completely disagree	largely disagree	slightly disagree	slightly agree	largely agree	completely agree
I like to occupy myself in greater detail with technical systems.	O	O	O	O	O	O
I like testing the functions of new technical systems.	O	O	O	O	O	O
It is enough for me that a technical system works; I don’t care how or why.	O	O	O	O	O	O
It is enough for me to know the basic functions of a technical system.	O	O	O	O	O	O

PAGE 09

13. Which gender do you most identify with?

- ○ female
- ○ male
- ○ non-binary
- ○ Prefer not to disclose

14. How old are you?

I am [ ] years old.

15. How good are your english skills?

- ○ A1, A2 level (Basic knowledge)
- ○ B1, B2 level (Good knowledge)
- ○ C1, C2 level (Very good/excellent knowledge

16. What is the highest level of education you have achieved as of today?

○ None.
○ Level 1 (e.g., GCSE (grades D, E, F or G), Level 1 certificates, equivalents)
○ Level 2 (e.g., GCSE (grades A*, A, B or C), O level (grades A, B or C), Grade 1 at CSE level, Level 2 functional or essential skills, equivalents)
○ Level 3 (e.g., A level, access to higher education diploma, level 3 certificate, level 3 certificate, equivalents)
○ Level 4 (Higher national certificate (HNC), certificate of higher education (CertHE), level 4 awards, equivalents)
○ Level 5 (Foundation degree, higher national diploma (HND), diploma of higher education (DipHE), equivalents)
○ Level 6 (Bachelor's degree (with or without honours), graduate diploma, equivalents)
○ Level 7 (Master's degree, integrated master's degree, postgraduate certificate in education (PGCE), equivalents)
○ Level 8 (Doctorate or PhD, equivalents)
○ Other:

PAGE 10

If you have chosen to link this survey to your Prolific account, please click the following link to confirm that you have fully processed and completed the survey. The credit will automatically be applied to Prolific:

[Prolific completion link]

Thank you very much for your participation. Your answers have been transferred, you can now safely close this browser window or tab.

Thank You Very Much for Filling Out This Survey :-)!

C SAMPLE EDUCATION LEVELS

Table T.1. Detailed overview of the distribution of the education levels

Education	*n*	%
None	1	0.1
Level 1 (e.g., GCSE (grades D, E, F or G), Level 1 certificates, equivalents)	9	1.1
Level 2 (e.g., GCSE (grades A*, A, B or C), O level (grades A, B or C), Grade 1 at CSE level, Level 2 functional or essential skills, equivalents)	68	8.6
Level 3 (e.g., A level, access to higher education diploma, level 3 certificate, level 3 certificate, equivalents)	119	15.0
Level 4 (Higher national certificate (HNC), certificate of higher education (CertHE), level 4 awards, equivalents)	35	4.4
Level 5 (Foundation degree, higher national diploma (HND), diploma of higher education (DipHE), equivalents)	35	4.4
Level 6 (Bachelor's degree (with or without honours), graduate diploma, equivalents)	339	42.7
Level 7 (Master's degree, integrated master's degree, postgraduate certificate in education (PGCE), equivalents)	154	19.4
Level 8 (Doctorate or PhD, equivalents)	32	4.0
Other:	1	0.1

D DISTRIBUTION OF RESPONSES OF DEPENDENT VARIABLES

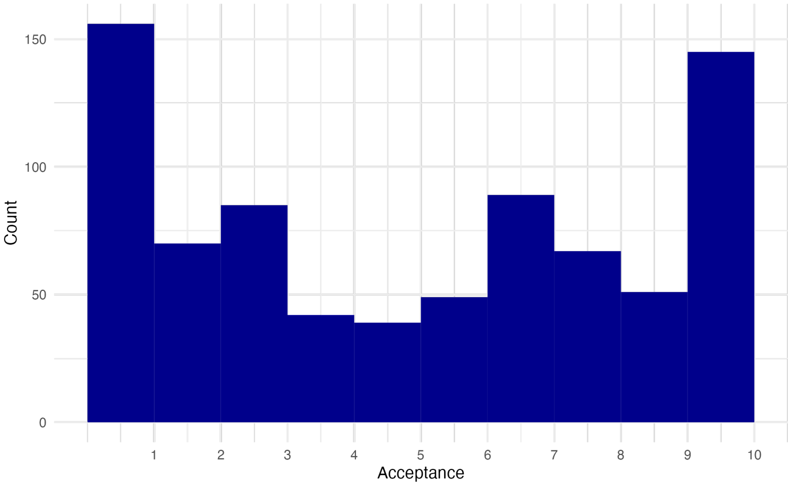


Fig. A.1. Distribution of responses on the acceptance scale of all vignettes

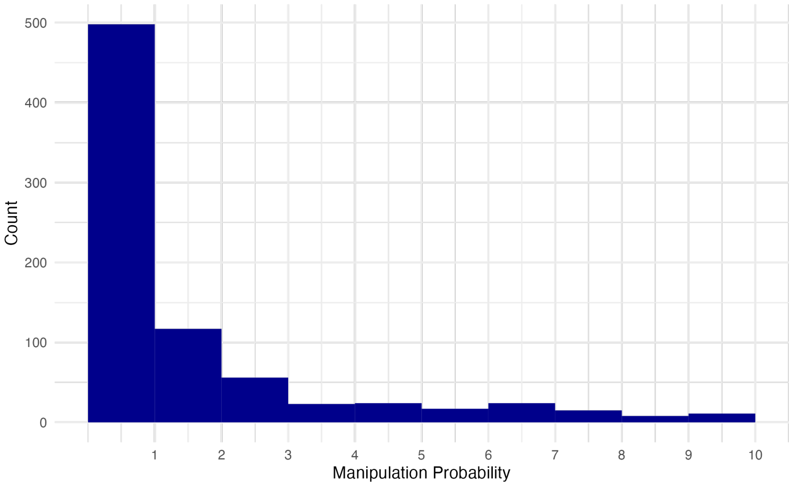


Fig. A.2. Distribution of responses on the manipulation probability scale of all vignettes

E CORRELATION TABLES OF INDEPENDENT VARIABLES ON THE MANIPULATION PROBABILITY

Table T.2. Correlation table of independent variables on acceptance

Variable	*M*	*SD*	1	2	3	4
1 Acceptance	5.39	3.34	-	.28**	-.32**	-.05
2 Consent				-	-.34**	-.01
3 Consequences	2.44	1.12			-	-.001
4 Incentive						-

N = 793, $^{*}p$ *<.05,* $^{**}p$ *<.01*

Table T.3. Correlation table of independent variables on manipulation probability

Variable	*M*	*SD*	1	2	3	4
1 Manipulation Prob.	2.12	2.06	-	.03	.06	.04
2 Consent				-	-.34**	-.01
3 Consequences	2.44	1.12			-	-.001
4 Incentive						-

N = 793, $^{*}p$ *<.05,* $^{**}p$ *<.01*

F OVERALL EFFECTS OF THE INDEPENDENT VARIABLES ON ACCEPTANCE/MANIPULATION PROBABILITY

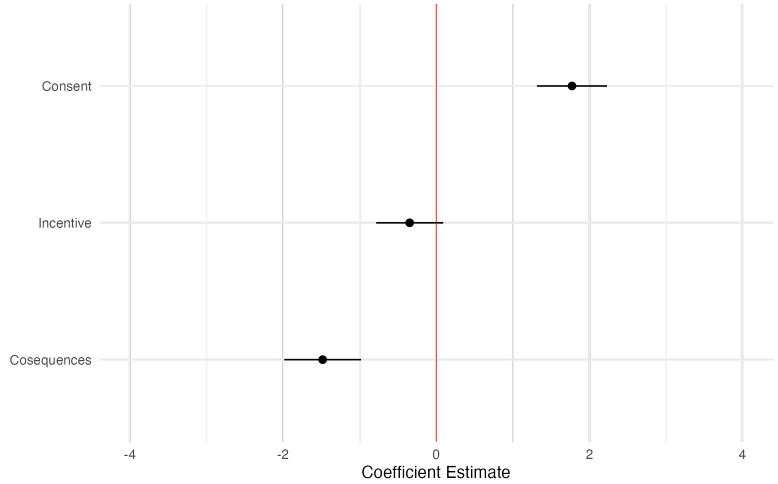


Fig. A.3. Overall effects of the independent variables on acceptance

Table T.4. Regression table overall effects on acceptance. Acceptance was measured on a scale of 1 to 10.

Term	Estimate	
(Intercept)	5.9972	(0.2665)
Consent	1.7731***	(0.2334)
Incentive	-0.3464	(0.2235)
Consequences (dummy)	-1.4830***	(0.2557)

Standard errors in parentheses

+ p < .10, * p < .05, ** p < .01, *** p < .001

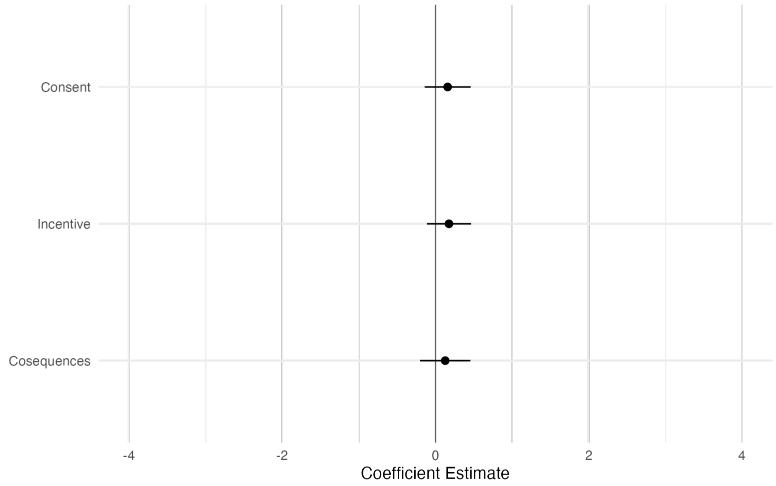


Fig. A.4. Overall effects of the independent variables on manipulation probability

Table T.5. Regression table overall effects on manipulation probability. Manipulation probability was measured on a scale of 1 to 10.

Term	Estimate	
(Intercept)	1.8898	(0.1748)
Consent	0.1587	(0.1531)
Incentive	0.1757	(0.1466)
Consequences (dummy)	0.1269	(0.1678)

Standard errors in parentheses

+ p < .10, * p < .05, ** p < .01, *** p < .001