What Motivates and Discourages Employees in Phishing Interventions: An Exploration of Expectancy-Value Theory

Xiaowei Chen[1], Sophie Doublet[1], Anastasia Sergeeva[1],
Gabriele Lenzini[1], Vincent Koenig[1], Verena Distler[2]
[1]*University of Luxembourg*
[2]*University of the Bundeswehr Munich*

Abstract

Organizations adopt a combination of measures to defend against phishing attacks that pass through technical filters. However, employees' engagement with these countermeasures often does not meet security experts' expectations. To explore what motivates and discourages employees from engaging with user-oriented phishing interventions, we conducted seven focus groups with 34 employees at a European university, applying the Expectancy-Value Theory. Our study revealed a spectrum of factors influencing employees' engagement. The perceived value of phishing interventions influences employees' participation. Although the expectation of mitigation and fear of consequences can motivate employees, lack of feedback and communication, worries, and privacy concerns discourage them from reporting phishing emails. We found that the expectancy-value framework provides a unique lens for explaining how organizational culture, social roles, and the influence of colleagues and supervisors foster proactive responses to phishing attacks. We documented a range of improvements proposed by employees to phishing interventions. Our findings underscore the importance of enhancing utility value, prioritizing positive user experiences, and nurturing employees' motivations to engage them with phishing interventions.

1 Introduction

Phishing was the most reported cybercrime in the U.S. between 2019 and 2022 [27]. Phishing emails deceive people into clicking on malicious links, disclosing sensitive information, or installing malware on their devices [2]. Phishing attacks endanger organizational intellectual property and institutional reputation, causing billions of losses [4, 27, 40]. Organizations employ a range of measures to defend against phishing attacks. Despite the implementation of technical filters, even if deep learning models achieve an accuracy rate of more than 96% [7, 33], a substantial number of phishing emails still end up in employees' inboxes. While technical solutions play a critical role in mitigating phishing attacks, employees are the last line of defense in organizations [55].

To raise employees' security awareness and educate them about phishing attacks, some organizations deploy online security courses as a cost-effective way to educate their employees [18]. Some organizations utilize simulated phishing tests in an attempt to track whether employees can identify phishing emails [10, 22]. Further, organizations broadly advocate for employees to report phishing emails, which enables IT teams to promptly detect incoming phishing attacks [52]. Research suggests that phishing interventions promote safe responses to attacks [49, 81], and reporting can serve as an effective crowd-sourced approach to counteract phishing [12, 52]. However, these user-oriented phishing interventions are not always embraced by employees [51, 62], as participation in the interventions requires time and effort and can interrupt the working routine [31, 47].

Motivation theories from educational psychology can be useful in explaining employee's (dis-)engagement. Recently, Expectancy-Value Theory (EVT) has received attention from scholars working in information management [68]. EVT seeks to explain individual behaviors with two central constructs: "expectation of success" and "subjective task value" [14]. We find these constructs particularly relevant and underinvestigated in security behavior studies [15].

In this paper, we examine employees' engagement with *phishing awareness campaigns*, which include online security courses and simulated phishing tests, as well as *reporting phishing emails* through the lens of EVT. By deepening understanding of the influencing factors associated with phishing interventions, organizations can improve their implementation

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.
August 11–13, 2024, Philadelphia, PA, United States.

of these interventions. We pursue the following objectives: 1) examining factors that motivate and discourage employees from engaging with phishing interventions, and 2) exploring what could be improved to increase employee engagement with these interventions. Focus groups are a qualitative method frequently applied to elicit ideas [79] and confront different viewpoints [78]. Educational institutions are frequently targeted by cybercriminals in recent years [53, 69]. Examining factors that influence university employees' engagement with phishing interventions is highly relevant to the current threat landscape. In light of this, we conducted seven focus groups with 34 employees (including research and non-research roles) in a European university.

Contributions. This paper makes empirical contributions, providing an enriched understanding of how various factors influence employee (dis-)engagement with phishing interventions. Our findings and adaptation of EVT suggest that it is a valuable theoretical framework for explaining how motivational factors influence employees' engagement with phishing interventions, highlighting its potential as a framework for future security behavior studies. This paper makes a theoretical contribution and highlights the possible adaptations to EVT for future use in organizational cybersecurity. Additionally, we offer practical suggestions for improving phishing awareness campaigns and reporting procedures in organizations, advocating user-centric approaches.

2 Related work

2.1 Phishing awareness campaigns

Simulated phishing tests are a tool for both assessment and educational purposes at organizations [22, 39]. Prior studies primarily utilized employees' click-through and reporting rates in phishing tests as indicators of employees' security behavior and their resilience to phishing attacks [22, 49, 81]. A recent case study highlighted that conducting simulated phishing tests at an organization requires significant time and effort from different stakeholders [8]. Moreover, some organizations have experienced side effects from phishing tests that have burdened CISO's relationship with employees [39]. When organizations neglect privacy concerns, fail to receive approval of simulated materials, don't specify the purpose of tests, or withhold appropriate feedback, it can lead to negative reactions from employees [62]. Phishing tests also increase employees' workload, potentially making them more susceptible to phishing attacks [8, 62]. Brunken et al. suggest involving employees in future research to better understand how simulated phishing tests impact them and their overall productivity at the workplace [8].

A variety of formats have been introduced to engage individuals with online security training [42]. Comic and game-based online trainings have reported notably high levels of satisfaction in user evaluations [50, 75]. A meta-analysis revealed that trainings combining text and comics demonstrated large effects in reducing victimization compared to comics or game-based trainings [9]. Online phishing quizzes, such as jigsaw puzzles, effectively improved participants' skills in detecting phishing emails [74]. Volkamer et al. created and evaluated a five-minute phishing awareness video, which significantly enhanced participants' ability to recognize phishing attempts both immediately and after an eight-week interval [72]. User feedback praised their video's clarity and simplicity, with suggestions for more phishing examples and a concluding summary [72]. Anti-phishing training utilizing storytelling led to higher levels of curiosity, self-efficacy and phishing detection ability than training employing comics in an online experiment [43]. To improve the effectiveness of security trainings, both the content and format of trainings were re-designed to engage learners.

While some studies suggest that offering educational materials after simulated tests improved employees' safe responses to phishing [49, 81], there are concerns about the effectiveness of this embedded training approach [8, 52]. Kumaraguru et al. found that employees who trained with anti-phishing materials after clicking links in simulated phishing emails exhibited a decreased likelihood of clicking on links in subsequent phishing tests compared to their untrained colleagues [49]. Yeoh et al. reported that the immediate provision of anti-phishing materials following phishing tests led to more safe responses than merely administering phishing tests [81]. Despite these findings, researchers suggested that only a small percentage of employees who clicked the phishing tests subsequently engaged with training materials [8, 20]. Thus, further investigation is required to better integrate simulated phishing tests and online security courses.

2.2 Phishing email reporting

Recent studies have begun to investigate factors that influence individuals' intention to report phishing emails. A survey with American college students [51] revealed that perceived self-efficacy, expected negative outcomes (*concern for mishandling of reports of spear phishing emails*), and cybersecurity self-monitoring increase the likelihood of reporting spear phishing emails. In alignment with [51], Kersten et al. suggested that user's intention to report phishing emails was negatively associated with the perceived "believability of the email" (the extent a user considers the email to be credible) in an online controlled experiment [46]. In an in-situ deception study [20], Distler found that employees' motivations for reporting phishing included improving email filters and receiving positive feedback. Obstacles to reporting entailed uncertainties regarding the reporting process and rationale, coupled with concerns about "getting colleagues into trouble" for sending legitimate emails that were misinterpreted as phishing attempts. Additionally, participants believed that

reporting became redundant once they had clicked on the link in a simulated phishing email [20]. In a survey with US workers, factors such as self-efficacy, subjective norms, and altruism tendencies increased reporting intention. Conversely, "sportsmanship" hinders individuals from reporting phishing emails [56]. Other than utilitarian motives, Franz proposed that the design features and risk indication influence participants' acceptance of reporting tools and suggested further research into the role of hedonic motives in the reporting process [30]. Additional factors may influence an individual's intention and behavior regarding the reporting of phishing emails, warranting further investigation.

2.3 Theoretical models applied to study user security behavior

Prior research on user security behaviors has frequently focused on fear appeals, as seen in studies that examine the constructs of Protection Motivation Theory (PMT) [36]. PMT explains protection behavior through two processes: threat appraisal and coping appraisal. In threat appraisal, people evaluate their perceived vulnerability and the perceived severity of a situation, while coping appraisal entails assessing response efficacy, self-efficacy, and response cost [58, 63, 70]. However, there are limitations and constraints in applying PMT to study user security behaviors. Originally constructed to explain health protection behaviors, PMT is based on the premise that the threat is relevant to the individual; however, this might not be the case in the information security context [57]. In a Relative Weight Analysis, attitude, personal norms & ethics, and normative beliefs demonstrated the highest effect sizes and relative importance in explaining security compliance behaviors, emphasizing employee psychological and ethical traits [15]. These constructs are not included in the theoretical model of PMT. To overcome the limitations of PMT, recent studies have begun to integrate constructs from other motivational theories to examine user security behaviors [36].

Expectancy-Value Theory (EVT) [23] is an influential motivation theory in educational psychology [38]. According to EVT, individuals' beliefs about how well they will do on an upcoming task and the subjective values they attributed to it influence their engagement with the task [25] (refer to Appendix A for the core constructs of EVT). EVT shares the same theoretical root as PMT, as both theories developed from Atkinson's expectancy-value model [63, 76]. EVT examines individuals' anticipation and subjective task values in educational contexts [76], whereas PMT employs fear appeals to motivate protective actions in health management [63]. However, EVT has rarely been applied to security behavior studies [15]. In an experiment incorporating EVT constructs, Jenkins et al. found that the highest levels of security behavior were associated with minimal technical controls (*number of passwords a participant was forced to use and remember*) combined with security education [44]. A recent structural modeling study that applied EVT revealed that achievement, along with intrinsic and extrinsic motivations, are determinants in explaining the motivational values associated with users' intention to protect mobile identity [3]. Applying EVT to investigate the factors that influence employee engagement with phishing interventions appears promising.

2.4 Research objectives

Low employee engagement with phishing interventions continues to be an obstacle to achieving information security in organizations [51, 81]. EVT has been utilized to examine learners' motivations in various contexts, including organizational [11, 41]. Applying EVT can elicit employees' motivational factors associated with phishing interventions. Further, beliefs and values form attitudes in the cognitive process, which in turn guide behavioral responses [44]. Expectation and subjective task values directly influence people's choices and performance in the EVT framework (see figure 1). Consequently, we propose to utilize EVT constructs to address the following research questions (**RQ**):

> RQ1: Which factors motivate employees to engage with phishing interventions?
>
> RQ2: Which factors discourage employees from engaging with phishing interventions?
>
> RQ3: From the employees' perspective, which aspects of phishing interventions could be improved?

3 Study design

We conducted focus groups with 34 employees at a European university to address these research questions. Focus groups are a form of interviewing where multiple participants come together to express and deliberate on their views regarding a predetermined topic in a collective discussion [21]. Focus groups are especially useful for gathering diverse and in-depth perspectives from interactions among participants [32, 78, 79], allowing us to gain an exhaustive understanding of the factors influencing employees' engagement with phishing interventions.

3.1 Study context

The study was conducted at a research-oriented European university that employs approximately 3,900 individuals. 38% of them are employed in research roles, whereas the remaining employees fulfill administrative functions. The organization uses a phishing awareness campaign sourced from a security service company. The IT team sends a simulated phishing test to all employees via the management software on a random

date each month. Employees who click the link or download the attachment within the phishing test land on a page displaying "you clicked on a simulated phishing test" and "rules to stay safe online". Afterwards, the IT team sends a web link to online security courses to those who responded unsafely. Employees who reported the simulated email to the IT team receive an automatic reply within a couple of minutes with the subject line "congratulations, you've spotted a phish".

To raise phishing awareness, the IT team sends every new employee an email during their first week that includes links to online security courses and suggested responses to suspicious emails. To defend the organization against phishing attacks, the IT team encourages employees to report any suspicious emails to "report-a-phish@anonymized". When the reported email is a simulated test, a program automatically sends out a reply; otherwise, a security expert manually reviews the reported email. Normally, it takes one or two working days for the expert to reply with the verification result of the reported email. When a reported email is a phishing attempt, the expert sends a phish alert to individuals who also received the phishing attempt. When the email is legitimate (not a phish), the expert replies with "It is a legitimate email".

At the time of our investigation, all employees automatically received simulated phishing emails as part of their cybersecurity training without prior informed consent. Employees could either actively engage by reporting the simulated test in accordance with the organization's suggestions for handling suspicious emails or ignore these simulated tests.

3.2 Participants

We used multiple approaches to recruit study participants, including posters across three administrative buildings, LinkedIn posts, email invitations, and direct outreach. Forty-five employees registered their interest in participating in our study. We assigned them to different groups based on the similarity of their job roles and the diversity of faculty. We did not exclude any specializations (e.g., computer scientists) when scheduling our focus groups. Due to personal reasons, 34 of the 45 interested employees participated in seven focus group sessions (20 female, 13 male, and one non-binary) between November 2022 and January 2023. Each session consisted of three to seven participants. Participants included 19 researchers, 12 administrative staff, and 3 software developers. On average, the research staff had worked at the organization for 1.3 years (SD=0.9), and the non-research staff 7.3 years (SD=6.7). The participants' age ranged from 25 to 56 years (mean=37.6, SD=10.8). In the demographic questionnaire, 32 (94%) participants indicated that they had encountered phishing attacks previously; 29 (85%) had received simulated tests from the IT team[1]; 25 (74%) had reported phishing emails to the IT department, and 14 (41%) had previously participated in online security courses. We include the participant demographic information in Appendix D.

3.3 Procedure

Prior to data collection, we conducted two pre-test sessions (N=11) to refine our protocol. During the first pre-test, we led the discussion using a synthesized framework of motivation theories [38]. Introducing concepts from multiple theories led to cognitive overload for participants during the focus group. In the second pre-test, we narrowed our focus to EVT. According to the preliminary analysis, observations, and participants' feedback on the pretests, we improved our discussion questions and added templates and brainstorming activities. The revised focus groups included four parts: a warm-up activity, a group discussion, a brainstorming activity, and the debriefing. Each focus group took approximately 90 minutes.

First, we conducted a warm-up activity to familiarize the participants with the lab and to elicit what motivates and discourages them from engaging with a self-selected leisure activity through **Template 1**. This stage lasted for 10 minutes.

In the second part, the participants were involved in a group discussion on phishing awareness campaigns for 25 minutes. Then, we instructed them to complete **Template 2** to record their motivating and discouraging factors for reporting suspicious emails. Following this, participants continued discussing the factors influencing their reporting. This stage planned a total of 60 minutes and included 12 questions to examine *general opinions, self-concept of their ability, goal setting*, and *role identification*, as well as their subjective task value (*costs, benefits*) related to participating in phishing interventions. These questions were adapted from the core concepts within EVT framework that affect individual's choices and performance (see Figure 1).

In the third part, participants were asked to brainstorm as if they were the new chief information security officer in response to an increase in phishing emails targeting the university. Participants were tasked with designing strategies to engage employees with phishing interventions in groups. This round lasted 15 minutes.

Lastly, the participants were debriefed by introducing the standard practices suggested by the IT department to avoid any misunderstandings caused by opinions mentioned during the discussion. We provide the **two templates** and full focus group **protocol** in Appendix B.

3.4 Data collection and analysis methods

We recorded audio and video of the focus group sessions. We used the audio recordings (11 hours in total) for the analysis[2]. The audio was transcribed automatically using Microsoft

[1] Every employee is scheduled to receive a phishing test monthly. These five employees, who reported not receiving any phishing tests, may have simply not clicked on or noticed the tests.

[2] Videos were recorded with the lab's default system as a backup resource in case of audio disruption and were deleted after transcription.

Word and reviewed to ensure accuracy. We pseudonymized the transcripts to protect the identity of participants prior to analysis.

The answers to "Template 2. What motivates/discourages you from reporting" were transcribed into an Excel spreadsheet. The first and second author then independently coded the template, following a thematic analysis procedure [13]. Then the two authors categorized the generated codes into preliminary groups in a discussion, which yielded an initial set of codes. Concurrently, a coding workshop was conducted with five researchers experienced in qualitative research and coding. This workshop, which employed an inductive approach [34], analyzed the transcripts from two focus group sessions. Consequently, a second set of codes was created. By integrating the template codes with those from the workshop, the first author established a code system in MAXQDA [71]. The code system was reviewed and revised by three authors. All transcripts were subsequently coded by the first author using MAXQDA. Theme saturation [59] was reached after completing the coding of data from the sixth group. The second author thoroughly reviewed all coded transcripts for consistency and accuracy. A few disagreements were resolved before the final summary of findings via discussion between authors and reviewing the context of the coded segments. We include our coding scheme in Appendix C.

3.5 Ethics

The study received approval from the university's ethics review board prior to the pretest. We emphasized that "the session is strictly confidential" to assert peer confidentiality in the email confirmation prior to each session. All participants were informed of their right to withdraw both during and after the study and provided informed consent. The raw data collected in this study were kept confidential to the researchers and stored in line with the General Data Protection Regulation (GDPR) and the ethical guidance of the research institution. Each participant received a €40 gift voucher as compensation for their 90-minute participation. We only used pseudonymized data for analysis.

4 Results

We present the factors thematically according to the core concepts of EVT framework and highlight those that could not be located within the framework (see Table 1). Unlike qualitative data from individual interviews and open-ended questionnaires, the factors emerging from focus group conversations represent a co-creation among participants. There were occasions when participants filled in specific factors in the template (e.g., P28: "being a good citizen") but did not mention them during discussions, or situations where a factor was articulated in depth by one participant, leading others to choose not to repeat it. Providing the frequency of each theme mentioned by participants would thus not be meaningful.

4.1 Phishing awareness campaigns

4.1.1 Factors that motivate employees

Gaining phishing knowledge and *enhancing phishing awareness* are the two utility values mentioned by many participants. They noted that the awareness campaign demonstrated that phishing attacks are constantly changing and evolving. They learned that it is critical to remain informed of evolving phishing techniques, which can support their decision-making in responding to suspicious emails. Additionally, phishing campaigns keep them vigilant of phishing attempts in their daily work. Not only beginners who were not tech savvy could benefit from the campaigns but also experienced employees could be reminded that they need to be cautious of contextual factors. As P2 stated, "even if you're aware of the problem and know how to check ... you can still fall for it (phishing test) if you don't pay attention, if there's a lot of stress and you're going faster." Additionally, a few participants considered participating in phishing campaign to be a game (P8), and some parts of the online training were "awesome" and "*fun*" (P26).

Acquiring skills in identifying whether emails are legitimate or not from awareness campaigns was mentioned by some participants as a motivating factor. Through the campaigns, they increase their competence (self-concept of one's ability). They perceived the phishing campaign as beneficial in "training people to recognize what is phishing and prevent them from actually falling into one when it happens" (P22). Consequently, they held this expectation of maintaining *cyber safety*. As P9 shared, the campaign not only benefited them in terms of protecting their own data and e-mail accounts, it also "helped the university as an institution to be better protected."

A few participants believed that receiving training on security-related knowledge could benefit their life and improve their computer literacy, contributing to *personal development* or long-term goals. P29 stressed that cybersecurity knowledge would become a fundamental skill for them to perform daily tasks with digital tools, and "it's not only about fear of being attacked, you need to understand what's inside these technology tools ... everything related to cybersecurity is very fundamental now and, in the future, would become even more fundamental, like reading."

4.1.2 Factors that discourage employees

Perceived low value discourages participants from taking online security courses, as indicated by P9, "not sure this kind of course will help me to be more precise in making judgments." On the one hand, the course was perceived as low value for some participants who had received security training before working in the current organization. On the other hand, some

Table 1: Motivational factors associated with phishing interventions.

	Phishing Awareness Campaigns		Report Phishing Emails	
	Motivating	**Discouraging**	**Motivating**	**Discouraging**
Expectation	Cyber safety	Optimism bias	Expectation of mitigating, Fear of consequences	Lack of feedback, Lack of communication
Utility value	Phishing knowledge, Phishing awareness	Perceived low value, Lack of incentive	Protecting oneself, Safeguarding the workplace	Low utility value
Intrinsic value	Fun	Lack of interest	Enjoyment, Satisfaction, Pride	
Attainment value		Other priorities	Core values	
Cost		Time constraint, Interrupting workflow, Opportunity cost, Negative inference	Easy to report	Usability issues, Worries and privacy concerns
Competence	Acquiring skills	Overconfidence	Empowerment	Low self-efficacy
Social identity			Recognition, peer influence, sense of belonging	
Goal	Personal development			
Self-schemata		Procrastination		Habitual behavior
Previous experience		Fear of failing the training	Phishing experience	
Outside of EVT				Contextual factors

participants had concerns that the course might be in technical language, which can be difficult for people who are not tech-savvy to understand, "I'm going to attend it, but I'm not going to understand it" (P13). Furthermore, participants shared that the *lack of incentives* discouraged them from participating in security course. If the organization offered incentives, such as course credits (for doctoral researchers), compensation, and praise from the team leader, they would be more likely to participate in the security courses. As P24 asked, "what is my incentive to do an optional course here?"

Some participants expressed that even though they had intended to learn from the security course, the cover image and name of the course gave them the impression that it would *not be interesting*, resulting in them disengaging with the courses (P16). Participants thought that the course exercises were too simple; "the exercises were so obvious that you would truly have to make an effort to answer wrongly" (P2).

Participants frequently mentioned *time as a constraint* that discourages them from engaging with awareness campaigns. Participants found it difficult to allocate time to the awareness campaign due to their packed schedules. Time spent on the campaign was seen as an *opportunity cost*, as P23 stated, "instead of achieving something for your project, for example, a good experimental result, you spend time on the phishing campaigns, and you lose that opportunity." Multiple participants shared that a downside to engaging with awareness campaigns was heightened worry about potential threats - "*Negative inference*" (P30). An awareness campaign might lead them to experience more stress, compelling them to exercise increased caution in their daily lives (P5 and P25).

Participants expressed less interest in the campaign if the course content was not relevant to their area of expertise or interests. "*Other higher priorities*, such as course work and the experiment, would discourage me from participating in the awareness course; for me, the security courses were super boring" (P23). Participating in awareness campaigns requires people to switch from their tasks at hand to phishing-related content. The switching *interrupted their workflow* (P25). Switching between tasks meant that it took additional hours for them to perform their duties (P27).

Participants' belief that they were less likely to experience phishing compared to others led to less involvement with the awareness campaign (*optimism bias*). As illustrated in P14's case, "I always had this thinking, it won't happen to me because this (phishing email) is so stupid." Participants also indicated that *overconfidence* in their knowledge of the topic

made them less likely to engage with the awareness campaign (P28).

Previous negative experiences with security courses might evoke a *fear of failing the training*, which discouraged employees from participating. As P8 shared, "the fear or the worry that if I failed the course, it would be tracked. Because I experienced that in the previous job. If you didn't get a certain grade, then you would be forced to retake it and retake it." Additionally, participants shared that *procrastination* resulted in delaying or forgetting to take the courses (P32 and P33).

4.2 Report phishing emails

4.2.1 Factors that motivate employees

Participants had specific *expectations* when they reported phishing emails. Reporting was a practical way of notifying colleagues and alerting them of phishing attempts. Participants expected that the organization would improve its spam filters with their reported emails, which would benefit them in terms of receiving fewer spam and phishing emails in future. "The main benefit of reporting is that the IT team could create more filters for phishing emails if they have more data (from reporting), making us safer" (P27). They expected that the organization could contain the damage, retrieve stolen data from attackers and mitigate risks. *Worries and fears* related to the consequences of phishing attacks prompt participants to report. Specifically, participants worried that they would get into trouble, lose information, suffer from financial risks, and involvement in cyber crimes if they did not report promptly. Several participants emphasized reporting to avoid potential reputational damage and financial losses for their workplace (P13).

Participants indicated that reporting *protected their personal data*, financial assets, and other valuable possessions, including personal accounts. When suspicious of an email, they received support from the IT department in assessing the reported email. Beyond work-related protection, one participant felt safer in their personal life after reporting a phishing attempt to law enforcement, specifically an email accusing them of financial misconduct. Their concerns were alleviated once the email was confirmed as a phishing attempt. Participants also regarded reporting as a measure to *safeguard the workplace*. Firstly, reporting phishing attempts protected the organization's confidential data, documentation, work tools, internal network and servers from external access (P23). Secondly, reporting was viewed as a way of raising awareness of phishing attempts in the organization. Not only the IT team needed to be notified of phishing attempts, but also their colleagues (P11 and P12). Thirdly, participants regarded reporting as a collaborative approach to countering phishing. The IT team assisted the employees in verifying the legitimacy of emails, and employees assisted the IT team in detecting the phishing attempts in real-time (P19).

Participants shared their *experiences receiving phishing emails*. Some received suspicious emails from professors, colleagues or family members asking for money or directing them to fraudulent websites. Others fell for phishing attempts while using online hotel booking platforms. P19 is a doctoral researcher in computer science who got phished a week before the focus group, "I lost two days of my life trying to correct just one click. During the backup, I lost a bunch of documents (erased a password for storing work documents), so there were other consequences after that." Even though the incident happened in their private life, it impacted their work. After the phishing incident, P19 wanted to warn others about phishing attacks and was motivated to report phishing attempts.

The ease of reporting phishing emails was mentioned as a reason why some participants reported phishing frequently. They referred to the one-click reporting button as straightforward, which made the reporting process simple and not time-consuming. They emphasize the one-click option for quick responses. The positive user experience of the reporting button facilitated participants to report, as exemplified by P31: "It's easy so it doesn't take even two seconds. If you suspect, click, click, and then you're done."

Participants regard the "congratulations" email that they received from the IT team when they reported a (simulated) phish as a kind of "*recognition*" and extrinsic reward for their reporting (P9). While P21 used to ignore phishing emails, one colleague told them it's better to report (*peer influence*). After that, P21 started to report suspicious emails. The *sense of being part of the community* prompts participants to report, as exemplified by the following conversation:

> P32: "We need to participate. We're all active users and it's not just IT who has to deal with it."
>
> P34: "We are actors within the community. So, we are together."

Participants described that they experienced feelings of *enjoyment, satisfaction*, and *pride* when reporting phishing attempts, likening the process to a game, feeling proud of their vigilance, and deriving a sense of satisfaction from reporting. As P28, P11, and P8 indicated:

> "When you click to report phishing attempts, then you receive 'congratulations'. I'm happy and it's like a game." (P28)
>
> "I can relate to the sense of satisfaction. Once you've reported it, you feel like you played your role. You did a good job." (P11)
>
> "I don't want to break my streak of always reporting the phishing attacks ... I'm quite proud of that." (P8)

Several participants mentioned a number of *core values* (guiding principles that shape people's attitudes, actions, and decisions) that drive them to report phishing attempts, including "help others" and "vulnerable" groups (P2 and P15), "duty"

(P11), "being a good citizen" (P28 and P33), and "contributing to the fight against phishing" (P33). Additionally, a few participants considered reporting as an approach to take control and make a difference (P6). In P16's case, "I had the initiative to defend against the phishing attack. And knowing that I can stop spreading this attack for other people and for my future self really helps me, like *empowering*."

4.2.2 Factors that discourage employees

Multiple participants felt discouraged from reporting suspicious emails because they received *no feedback* on the outcome of their actions. They expected to receive more information about the outcomes of their reporting (P12). As P31 emphasized, "we don't know what the effectiveness of reporting phishing emails is. We don't know the numbers, so it would be really good to have a kind of feedback status. What has been done last year? What was the success rate?" Further, even for participants who reported diligently, they sometimes felt discouraged from reporting due to not knowing whether their colleagues were reporting or not (*lack of communication*).

> "I report phishing emails regularly and religiously, but I'm thinking is everyone else doing the same as me, putting in the same effort as I am on reporting? It takes maybe 30 seconds of your time, but I'm still very careful about it." (P25)

The perceived *low utility value* discouraged participants from reporting phishing emails. Firstly, the belief that the "phishing" email is merely a test from the IT department reduces the perceived need to report it, as stressed by P27, "for me, every phishing email that I received was a simulated one. So, I didn't see the point of reporting that because I knew that it was from IT." Secondly, if the participants believed most people would be able to recognize the email as a phish and posited a low threat to others, they chose not to report (P16). Thirdly, worries of additional burden due to reporting discouraged participants from following the reporting procedure. These assumed negative outcomes included "bog me down with questions" (P13), getting "more emails" (P17), and "fear of annoying IT staff" (P28). Lastly, the belief that reporting doesn't lead to effective outcomes, such as prevention or resolution of the attack, discouraged participants from reporting. As exemplified by P19, "the lack of results discourages me. It seems like we try to do something nice and nobody really cares."

Participants highlighted several issues related to ease of use, functionality, and efficiency in the reporting process as discouraging factors (*usability issues*). Some participants found the reporting procedures ambiguous. For instance, P8 only learned about the "report-a-phish" email address from a colleague after observing the absence of a reporting button following an update of the email client. P26 wondered about the preferred method of reporting, stating, "I forwarded it to report-a-phish, and they said, 'Oh no, can you please send it as an attachment instead of forwarding it'." For participants who frequently reported suspicious emails on their laptops mentioned that they often delete or disregard such emails when viewed on their smartphones. P9 shared, "I wanted to report it and I had trouble doing that with my phone. So I always try to be extremely careful, almost like you have something burning in your hand." Despite their caution, they still accidentally clicked on the email when trying to report it, leading them to ignore phishing emails on their phones. Moreover, Linux and Mac OS users felt the reporting process demanded too much effort. It's easier to just delete the suspicious email than to forward the email as an attachment to the IT department. As emphasized by P24, "if it's anything more than a one-button click would be a little bit more discouraging."

Participants expressed they would not report when they were concerned that the suspicious emails "*disclose their private information*" or cause false impressions about their personal life (P4, P28). Additionally, *worries about being judged* by the IT team were shared as a discouraging factor by participants. As the conversation between P33 and P34 revealed:

> P34: "I have this feeling that IT guys, they're always like a bit, 'they don't know they're doing really.' And I feel I'm so stupid. If I report Netflix or something as phishing, then they would think 'stupid woman'."
>
> P33: "They could judge us."
>
> P34: "So this feeling unnerved me and discouraged me from reporting. Because they give you this feeling sometimes. I experience it, I call the help desk and get this 'again'."

Participants shared that they frequently postponed or forgot to report because they reverted to their *old habits* of simply deleting emails. They mentioned that the reporting process is unique to their current workplace, contrasting it with their usual habit of deleting or marking suspicious emails as spam. As P11 stated, "in my personal life, when I encounter a suspicious email, I just delete or mark it as spam. However, this report-a-phish button is quite specific and new." Participants noted that if they *lacked confidence* in identifying whether an email is phishing, they would typically ignore it. Furthermore, some participants cited "laziness" as a reason for not reporting.

Contextual factors, such as task overload, stress, and time pressure, could deter participants from reporting phishing emails. When focused on one's tasks and in the status of flow, they perceived incoming emails as a distraction, resulting in less intention to report (P27).

4.3 Improvements proposed by participants

Participants proposed various ideas to make phishing interventions more engaging during the brainstorming sessions. We categorized them into the following themes:

Gamification elements: Participants suggested adding achievement, competition, virtual reputation, and fun elements to the reporting process. There should be rewards or acknowledgments for the department that actively participates in awareness campaigns and reports the most phishing emails. Participants recommended providing incentives for participation in phishing campaigns, such as gifts, praise, and course credits. Participants suggested that role-playing and leaderboards would engage employees with the security training.

New employees & Mandatory training: During the onboarding week for new employees, the university should provide a mandatory training session to equip them with knowledge about phishing and the reporting procedure. The IT team should walk in the shoes of new employees and find out the potential attack points within their work activities. Participants also suggested making a security course mandatory for frequent clickers of phishing tests and for departments that receive a high number of phishing attacks.

User experience: Participants suggested to improve the user experience of phishing interventions. Real-time verification of reported emails and shorter, more relevant and interactive trainings would attract employees. Course content should be personalized according to different levels of phishing knowledge. Participants suggested using pop-up quizzes instead of online videos to raise phishing awareness because the latter took too much time.

Communication: Participants suggested that the IT team provide regular updates or host information sessions with employees. The positive impacts that phishing interventions have on the university should be communicated quarterly or annually. Seminars drawing from diverse expertise areas like IT, HR, and research were recommended to bolster organizational defense and collaborations between departments.

Feedback: The IT team should gather feedback on phishing interventions from employees, provide statistics on phishing interventions, and be transparent about the state of the art and the efficacy of current solutions. Participants also suggested the IT team provide individual feedback on what happens after an employee reports phishing.

Present real incidents: Participants suggested the IT team present real phishing attacks and their consequences as examples to raise awareness. Providing concrete examples of how data breaches happened through phishing would raise employees' phishing awareness.

Authentication of internal emails: Participants suggested implementing digital signatures to authenticate internal communication, which would enable fast detection of phishing emails that masquerade as internal communication. Additionally, participants suggested recruiting *more IT employees* to host training sessions regularly, noting that the IT team seems occupied with an overload of tasks. Lastly, one group proposed a *punishment* approach, that is, increasing the number of simulated phishing emails for employees who repeatedly clicked simulated phishing emails.

5 Discussion

5.1 Applying EVT to the context of organizational cybersecurity behaviors

In this study, we investigate how Expectancy-Value Theory (EVT) can illuminate the factors influencing employees' engagement with phishing interventions. Building on our findings and considering that EVT was created to interpret achievement-related choice and performance in educational settings, we propose incorporating an organizational dimension into EVT model (refer to Figure 1, our adaptations to EVT are in blue italics). Hence, we suggest integrating the organizational dimension in the form of "organizational culture" [80] into a "cultural milieu" construct, which can be described as a system of social roles, each with its associated responsibilities and obligations [77]. Perception of the organizational dimension can be interpreted through the lens of the "psychological contract", which refers to an unwritten set of expectations and beliefs about the obligations that exist between an employee and their employer [35], also including employees' beliefs about their responsibilities in organizational security [37]. During group discussions, employees consistently highlighted that, through their security behaviors, they aim to collaborate with the IT department in fighting against phishing attacks and safeguarding the organization. Despite the absence of explicit organizational policies dictating such obligations, this inclination can be attributed to the implicit norms acquired through the organization's unspoken rules and in general - organizational culture as a proxy for information security culture in the organization [66]. Our results suggest that the perception of the organizational culture, communicated through socializers' beliefs and behaviors, can contribute to a constructive "us vs. them" (organization vs. attackers) mentality, where employees have a self-concept of a contributor to organizational security.

In accord with past studies [19, 73], we observe that "peer influence" and "knowledge sharing" among colleagues influence employees' intention to report phishing emails and participate in online security courses. Pursuing this line of thought, we can extend the EVT model's "socializer" construct to include "colleagues and supervisors." These people convey their knowledge of the organization's unwritten norms to other employees, aiding in shaping security protective identities. Furthermore, we propose that employees' security consciousness stems from their social identity in EVT. Being a "responsible" employee dedicated to the organization, in harmony with other foundational roles, makes up one's social

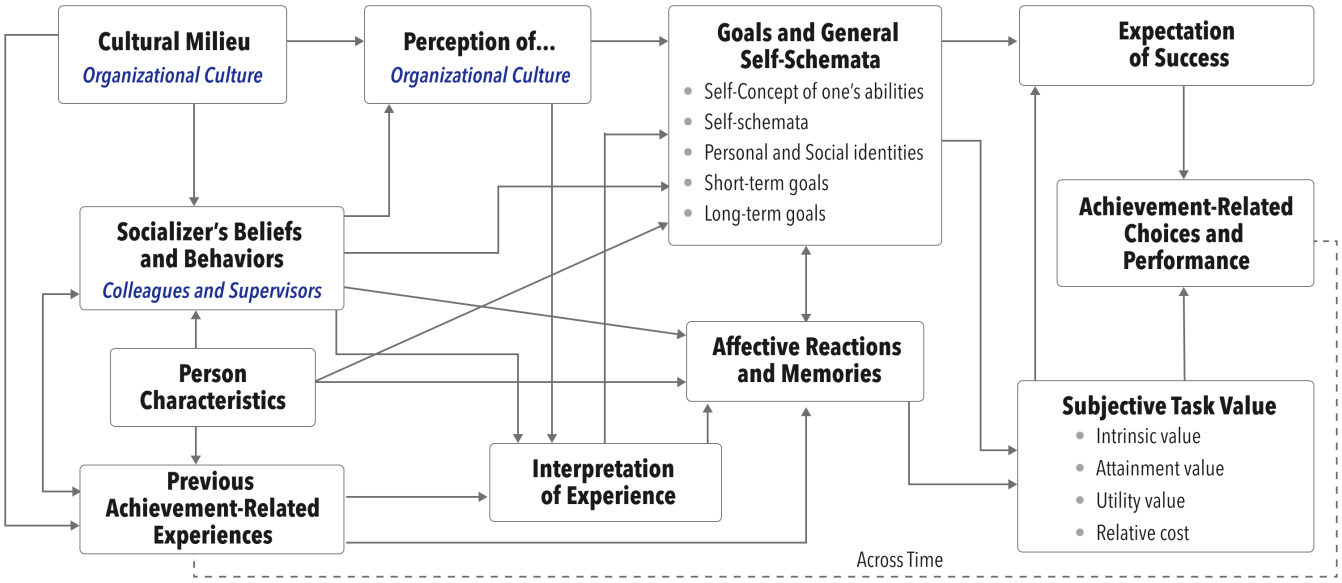

Figure 1: The expectancy-value model (adapted from [25]).

identity. This is connected with the "extra-role security behaviors" phenomenon [29, 54], in which some employees are self-motivated to take additional responsibilities to secure the organization, even if these responsibilities go beyond their contractual role. In our study, we found strong evidence that this type of motivation is one of the core drivers of reporting phishing emails.

In summary, our empirical findings demonstrate that the EVT framework can be specialized for use in organizational security settings. We specify certain concepts of EVT in the organizational setting, proposing to focus on the organizational culture, colleagues and supervisors, and "previous experience" on the left side of the framework (see Figure 1). Our findings also support the original EVT framework with findings that subjective task values, expectations, goals, and general self-schemata influence employees' engagement with phishing interventions. The discovery paves the foundation for future studies to apply EVT in studying organizational security behaviors.

5.2 Subjective task value of phishing interventions

The majority of educational interventions based on EVT focus on altering individuals' "Subjective task value" [26]. Subjective task value is the core construct within EVT, in which the value of engaging with an activity can be considered as the ratio between perceived benefits and associated costs [25]. People tend to opt for activities that have a higher benefit-to-cost ratio. Our findings showed that many of the discouraging factors of phishing awareness campaigns are associated with different types of costs, such as psychological cost, time cost, and opportunity cost. The findings align with previous studies on imposing security measures within organizations, which found that employees perceived the security measures as extra burdens that encumber their work [8, 47, 62]. Previous literature proposes remedies such as reducing the friction associated with security measures and automating security protocols [16, 31].

In the EVT framework, another promising avenue for exploration emerges: the potential for security managers to tip the scale in favor of security measures by reducing their associated costs. This shift could engage employees more with security measures. This idea aligns with studies showing positive outcomes from security trainings in short video format, with participants regarding the training "informative"/"useful" [82] and expressing interest in extended sessions [72]. The increased benefit-to-cost ratio in such cases can be attributed, in part, to the brevity and density of the training content. Our study echoes employee preferences for succinct training, as exemplified by "don't give me a half hour course for two minutes' value" (P13) in the group discussion. Similarly, participants in different groups proposed providing employees with shorter but more frequent security trainings.

Our study identifies a cluster of motivators associated with the intrinsic values of reporting. These motivators, deeply embedded in employees' psychological needs and desires, include satisfaction, empowerment, and core values (citizenship and altruism). Our findings are congruent with previous studies, which suggest that autonomy, personal values and principles influence users' security behavior [48, 57]. These elements, often sidestepped in security behavior research,

weave a complex network of factors influencing phishing reporting intentions. Considering that security messages that appeal to individuals' desires are more likely to elicit secure responses than those based on fear [57, 67], organizations should establish reporting procedures that resonate with employees' psychological needs. Integrating "fun" [65] and "experiential learning" [12] elements into training programs can enhance their intrinsic value, thereby engaging employees with phishing awareness campaigns. Furthermore, Eccles and Wigfield suggested developing attainment value-based interventions [26]. These interventions could take the approach of informing employees about the connection between anti-phishing practices and their personal values.

5.3 Previous experience, expectation of success, and personal development

Our study reveals that even motivated employees can become disheartened if they lack clear feedback and perceive their actions as ineffective. Several discouraging factors for phishing interventions can be categorized under "previous achievement-related experience." According to EVT, the "interpretation of experience" can influence "expectation of success" by altering goals and subjective task value. This attenuation is often due to negative experiences from prior engagement with the task. Employees are more inclined to adhere to security protocols if they deem the processes effective in mitigating phishing attacks [65]. Various employees in our study identified the lack of feedback and clarity about subsequent steps after reporting an email as discouraging factors, often provoking uncertainty and negative emotions. Such a phenomenon was also observed in employees' attitudes towards phishing awareness campaigns where previous unfavorable experiences shaped their perceptions. Over the last 20 years, research has persistently emphasized the critical role of feedback in fostering secure behavior within organizations [1, 6, 64]. Our study further explores the mechanisms through which an absence of feedback can alter motivation, even for motivated employees.

Intriguingly, we noted that prior experiences with being phished emerged as a strong motivator for some employees to report phishing, propelling their goal to prevent others from undergoing similar negative consequences. We hypothesize that the negative experience altered the subjective value they placed on reporting, which necessitates further study of this transformation from victim to defender in the context of phishing. Recognizing this transformative process can inform the development of support structures within the workplace. Employees who encounter cybersecurity incidents often experience guilt and shame. Workplaces should provide support, instead of blaming, to contain damage caused by the incidents and empower their employees [20, 61].

Employees demonstrated interest in acquiring security-related knowledge, linking it with their personal and professional growth. This interest suggests a pathway for organizations to refashion their security training to better align with employees' long-term goals. Given that all employees manage valuable accounts and passwords, and are often influenced by media reports or personal experiences of cybersecurity incidents, the imperative to adeptly navigate digital protection is clear. Similarly, Reeves et al. suggest shifting from a compliance-driven to a user-driven approach in security training to enhance the efficacy of training programs [60]. Incorporating employees' personal learning needs into organizational training paradigms could motivate employees to engage with security trainings.

5.4 Practical implications

We found that many of the discouraging factors related to the phishing awareness campaign are associated with its perceived value. Several usability-related factors discourage employees from reporting phishing emails. Fear, worries, and concerns about phishing interventions discourage employees from engaging (see Table 1). Leveraging insights from both the employee-generated suggestions and the EVT framework, we have proposed several improvements:

For phishing awareness campaigns: Clear communication of the campaign guidelines, expectations, goals, and consequences can alleviate the discouraging factor of "fear of failing training." Specific time slots should be allocated for employees to participate in the training sessions, addressing the discouraging factors of time constraints and interruption to their workflow [79]. This might not be possible in the case of knowledge workers who autonomously allocate time and tasks, for whom training will inevitably cut into their "productive" time. Making the training content relevant to individual job roles would enhance its relevance and applicability to daily tasks. Regular updates on evolving phishing attacks should be provided to increase awareness among employees. Gamification elements in the training program might enhance engagement [65].

For reporting phishing emails: Organizations should clearly communicate how reported incidents are managed by the IT team [28]. Timely feedback mechanisms should be established, reinforcing employees' sense of contributing to security. Regular updates (e.g., intranet, messages, displays) are beneficial for keeping employees informed about security efforts and emerging threats. Providing statistics on reporting and organizational benefits can underscore the personal value of reporting incidents. The reporting process should be frictionless to alleviate usability concerns. Ongoing awareness initiatives can foster engagement [17]. Training new employees is crucial to acquaint them with countering phishing practices and maintain a consistent level of awareness throughout the organization.

6 Limitations and future work

Despite their advantages, focus groups have a few limitations which we were careful to mitigate through purposeful moderation. The discussion might veer into narratives outside the scope of research. Also, dominant speakers might hijack the discussion while some participants might remain silent and not willing to confront others. This requires researchers' facilitation to steer back to the planned agenda and engage participants with contributing. Furthermore, much of the collected data is expressed informally, necessitating careful interpretation by researchers. Thus, we involved multiple researchers in the data analysis process. Participants' viewpoints might be influenced by the others' arguments during group interaction. Thus, we recorded individual opinions prior to the group discussion on reporting to obtain individual viewpoints.

Although we utilized diverse strategies to recruit employees from the organization, we might have attracted people who are particularly interested in the topic. We hypothesized that an important power imbalance exists between the IT security team and other staff regarding the topic of the study. We did not have IT security officers as participants. We acknowledge that focus groups were composed of participants with multiple roles, potentially creating a perceived power imbalance that inhibited participation. The investigated university has no strict rules regarding phishing awareness campaigns, reporting, and the use of personal devices for work. Thus, while our findings offer valuable insights, critical interpretation is warranted when extrapolating results to different organizational contexts. Future studies should use quantitative methodologies to test the hypotheses drawn from our results.

We found that contextual ("situated") factors, such as task overload, time pressure and stress, influence employees' response to phishing emails (in line with [20]). Contextual factors are not represented in the original EVT framework, although the authors later highlighted that the processes underlying the EVT model are influenced by the immediate situation in which a decision occurs [25]. Recent early-stage work suggests using knowledge about momentary user states to better tailor security interventions [5], for example proposing security interventions or training in opportune moments. We suggest future studies investigate how to integrate contextual factors into EVT when applying it to study information security behaviors.

7 Conclusion

Employees are the last line of organizational defense against phishing attacks [83]. It is important to train and engage employees and encourage reporting of phishing attacks to enable organizations to respond promptly. This engagement can be achieved by enhancing the perceived value of the task, reducing its relative costs, and making *phishing awareness campaigns* more user-centric and relevant to employees.

We find that Expectancy-Value Theory is a valuable theoretical framework for studying user security behavior in an organizational context. EVT helps explain how organizational culture, social roles, and the influence of colleagues and supervisors foster proactive responses to phishing attacks.

Our study reveals a spectrum of factors that influence employees' intentions to *report phishing emails*. Some factors not previously discussed in phishing studies include those associated with social roles (safeguarding the workplace, sense of belonging, and collaboration with IT) and intrinsic factors (satisfaction, enjoyment, and empowerment). Among the factors discouraging employees, the absence of feedback and perceived low utility value are particularly detrimental. This lack not only affects the perceived value of reporting but also undermines employees' confidence in the effectiveness of countermeasures. Given that users devote considerable time and effort in addition to their role to engage in security tasks, it seems justifiable to provide them with more feedback about how their actions fortify the organization's defenses against phishing attacks. A month after our focus group session, we received an email from P18—a highly motivated employee who indicated that they always report suspicious emails. They allowed us to cite:

> *I have now finally stopped reporting phishing emails. Yesterday, I received two that were exactly like the ones I've been getting dozens of times over the past years. It feels a bit like an insult to be asked to report phishing emails when this information is so evidently not utilized. I expressed this sentiment in my final report, but of course, it was ignored.*

We see this loss of engagement with phishing reporting as an understandable but regrettable behavioral response. Envisioning such sentiments and the resulting behavior at scale, with possibly large numbers of employees ending up disappointed and disengaging from phishing interventions, we can only speculate regarding the negative effects on the organizational security of an organization. We hope that this paper can help avoid such frustrating experiences for employees in the future by providing a better understanding of the motivating and discouraging factors for phishing interventions through the lens of EVT.

Acknowledgments

Author 1 acknowledges the financial support of the Institute for Advanced Studies at the University of Luxembourg through a Young Academic Grant (2021). The study was supported by the User Lab of the University of Luxembourg. Thank you to our reviewers for their constructive feedback. We thank all our participants. A shout-out to Eric J. Francois for his suggestion of role-playing, which inspired the development of a subsequent "role-playing as hackers" training [12].

References

[1] ADAMS, A., AND SASSE, M. A. Users are not the enemy. *Communications of the ACM 42*, 12 (1999), 40–46.

[2] ALEROUD, A., AND ZHOU, L. Phishing environments, techniques, and countermeasures: A survey. *Computers & Security 68* (2017), 160–196.

[3] ALHELALY, Y., DHILLON, G., AND OLIVEIRA, T. When expectation fails and motivation prevails: the mediating role of awareness in bridging the expectancy-capability gap in mobile identity protection. *Computers & Security 134* (2023), 103470.

[4] ALKHALIL, Z., HEWAGE, C., NAWAF, L., AND KHAN, I. Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science 3* (2021), 563060.

[5] ALT, F., HASSIB, M., AND DISTLER, V. Human-centered behavioral and physiological security. In *Proceedings of the 2023 New Security Paradigms Workshop* (New York, NY, USA, 2023), NSPW '23, Association for Computing Machinery, p. 48–61.

[6] BADA, M., SASSE, A. M., AND NURSE, J. R. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672* (2019).

[7] BAGUI, S., NANDI, D., BAGUI, S., AND WHITE, R. J. Machine learning and deep learning for phishing email classification using one-hot encoding. *Journal of Computer Science 17* (2021), 610–623.

[8] BRUNKEN, L., BUCKMANN, A., HIELSCHER, J., AND SASSE, M. A. "To Do This Properly, You Need More Resources": The Hidden Costs of Introducing Simulated Phishing Campaigns. In *32nd USENIX Security Symposium (USENIX Security 23)* (2023), pp. 4105–4122.

[9] BULLEE, J.-W., AND JUNGER, M. How effective are social engineering interventions? a meta-analysis. *Information & Computer Security 28*, 5 (2020), 801–830.

[10] BURNS, A., JOHNSON, M. E., AND CAPUTO, D. D. Spear phishing in a barrel: Insights from a targeted phishing campaign. *Journal of Organizational Computing and Electronic Commerce 29*, 1 (2019), 24–39.

[11] CHANG, C. L.-H., CHEN, V., KLEIN, G., AND JIANG, J. J. Information system personnel career anchor changes leading to career changes. *European Journal of Information Systems 20*, 1 (2011), 103–117.

[12] CHEN, X., SACRÉ, M., LENZINI, G., GREIFF, S., DISTLER, V., AND SERGEEVA, A. The effects of group discussion and role-playing training on self-efficacy, support-seeking, and reporting phishing emails: Evidence from a mixed-design experiment. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (2024), pp. 1–21.

[13] CLARKE, V., AND BRAUN, V. Thematic analysis. *The journal of positive psychology 12*, 3 (2017), 297–298.

[14] COOK, D. A., AND ARTINO JR, A. R. Motivation to learn: an overview of contemporary theories. *Medical education 50*, 10 (2016), 997–1014.

[15] CRAM, W. A., D'ARCY, J., AND PROUDFOOT, J. G. Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *MIS quarterly 43*, 2 (2019), 525–554.

[16] CRANOR, L. F. A framework for reasoning about the human in the loop.

[17] DA VEIGA, A., ASTAKHOVA, L. V., BOTHA, A., AND HERSELMAN, M. Defining organisational information security culture—perspectives from academia and industry. *Computers & Security 92* (2020), 101713.

[18] DAHABIYEH, L. Factors affecting organizational adoption and acceptance of computer-based security awareness training tools. *Information & Computer Security 29*, 5 (2021), 836–849.

[19] DANG-PHAM, D., KAUTZ, K., HOANG, A.-P., AND PITTAYACHAWAN, S. Identifying information security opinion leaders in organizations: Insights from the theory of social power bases and social network analysis. *Computers & Security 112* (2022), 102505.

[20] DISTLER, V. 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* (2023), pp. 1–18.

[21] DISTLER, V., FASSL, M., HABIB, H., KROMBHOLZ, K., LENZINI, G., LALLEMAND, C., KOENIG, V., AND CRANOR, L. F. Empirical research methods in usable privacy and security. In *Human Factors in Privacy Research*. Springer International Publishing Cham, 2023, pp. 29–53.

[22] DODGE JR, R. C., CARVER, C., AND FERGUSON, A. J. Phishing for user security awareness. *computers & security 26*, 1 (2007), 73–80.

[23] ECCLES, J. Expectancies, values and academic behaviors. *Achievement and achievement motives* (1983).

[24] ECCLES, J. S., AND WIGFIELD, A. Motivational beliefs, values, and goals. *Annual review of psychology 53*, 1 (2002), 109–132.

[25] ECCLES, J. S., AND WIGFIELD, A. From expectancy-value theory to situated expectancy-value theory: A developmental, social cognitive, and sociocultural perspective on motivation. *Contemporary educational psychology 61* (2020), 101859.

[26] ECCLES, J. S., AND WIGFIELD, A. The development, testing, and refinement of eccles, wigfield, and colleagues' situated expectancy-value model of achievement performance and choice. *Educational Psychology Review 36*, 2 (2024), 1–29.

[27] FBI. Internet crime report 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf, 2023. Accessed: 10-02-2024.

[28] FORMOSA, P., WILSON, M., AND RICHARDS, D. A principlist framework for cybersecurity ethics. *Computers & Security 109* (2021), 102382.

[29] FRANK, M., AND KOHN, V. Understanding extra-role security behaviors: An integration of self-determination theory and construal level theory. *Computers & Security 132* (2023), 103386.

[30] FRANZ, A. Why do employees report cyber threats? comparing utilitarian and hedonic motivations to use incident reporting tools. In *ICIS 2022 Proceedings* (2022), pp. 1–13.

[31] FRANZ, A., ZIMMERMANN, V., ALBRECHT, G., HARTWIG, K., REUTER, C., BENLIAN, A., AND VOGT, J. Sok: Still plenty of phish in the sea—a taxonomy of user-oriented phishing interventions and avenues for future research. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)* (2021), pp. 339–358.

[32] FUJS, D., MIHELIČ, A., AND VRHOVEC, S. L. The power of interpretation: Qualitative methods in cybersecurity research. In *Proceedings of the 14th International Conference on Availability, Reliability and Security* (2019), pp. 1–10.

[33] GHAZI-TEHRANI, A. K., AND PONTELL, H. N. Phishing evolves: Analyzing the enduring cybercrime. *Victims & Offenders 16*, 3 (2021), 316–342.

[34] GIOIA, D. A., CORLEY, K. G., AND HAMILTON, A. L. Seeking qualitative rigor in inductive research: Notes on the gioia methodology. *Organizational research methods 16*, 1 (2013), 15–31.

[35] GUEST, D. E., AND CONWAY, N. Communicating the psychological contract: an employer perspective. *Human resource management journal 12*, 2 (2002), 22–38.

[36] HAAG, S., SIPONEN, M., AND LIU, F. Protection motivation theory in information systems security research: A review of the past and a road map for the future. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems 52*, 2 (2021), 25–67.

[37] HAN, J., KIM, Y. J., AND KIM, H. An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security 66* (2017), 52–65.

[38] HATTIE, J., HODIS, F. A., AND KANG, S. H. Theories of motivation: Integration and ways forward. *Contemporary Educational Psychology 61* (2020), 101865.

[39] HIELSCHER, J., MENGES, U., PARKIN, S., KLUGE, A., AND SASSE, M. A. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *32nd USENIX Security Symposium (USENIX Security 23)* (2023), pp. 2311–2328.

[40] HOBBS, A. The colonial pipeline hack: Exposing vulnerabilities in us cybersecurity. In *SAGE Business Cases*. SAGE Publications: SAGE Business Cases Originals, 2021.

[41] HOSSEINI, M., ABDOLVAND, N., AND HARANDI, S. R. Two-dimensional analysis of customer behavior in traditional and electronic banking. *Digital Business 2*, 2 (2022), 100030.

[42] HU, S., HSU, C., AND ZHOU, Z. Security education, training, and awareness programs: Literature review. *Journal of Computer Information Systems 62*, 4 (2022), 752–764.

[43] HULL, D. M., SCHUETZ, S. W., AND LOWRY, P. B. Tell me a story: The effects that narratives exert on meaningful-engagement outcomes in antiphishing training. *Computers & Security 129* (2023), 103252.

[44] JENKINS, J. L., DURCIKOVA, A., ROSS, G., AND NUNAMAKER JR, J. F. Encouraging users to behave securely: Examining the influence of technical, managerial, and educational controls on users' secure behavior. In *ICIS 2010 Proceedings. 150.* (2010).

[45] KENDZIERSKI, D., AND WHITAKER, D. J. The role of self-schema in linking intentions with behavior. *Personality and Social Psychology Bulletin 23*, 2 (1997), 139–147.

[46] KERSTEN, L., BURDA, P., ALLODI, L., AND ZANNONE, N. Investigating the effect of phishing believability on phishing reporting. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (2022), IEEE, pp. 117–128.

[47] KIRLAPPOS, I., PARKIN, S., AND SASSE, M. A. Learning from "shadow security": Why understanding non-compliance provides the basis for effective security. In *Proceedings of Workshop on Usable Security 2014* (2014).

[48] KRANZ, J., AND HAEUSSINGER, F. Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior. In *International Conference on Information Systems* (2014), IEEE, pp. 1–14.

[49] KUMARAGURU, P., CRANSHAW, J., ACQUISTI, A., CRANOR, L., HONG, J., BLAIR, M. A., AND PHAM, T. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (2009), pp. 1–12.

[50] KUMARAGURU, P., RHEE, Y., SHENG, S., HASAN, S., ACQUISTI, A., CRANOR, L. F., AND HONG, J. Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. In *Proceedings of the Anti-Phishing Working Groups 2nd Annual ECrime Researchers Summit* (New York, NY, USA, 2007), eCrime '07, Association for Computing Machinery, p. 70–81.

[51] KWAK, Y., LEE, S., DAMIANO, A., AND VISHWANATH, A. Why do users not report spear phishing emails? *Telematics and Informatics 48* (2020), 101343.

[52] LAIN, D., KOSTIAINEN, K., AND ČAPKUN, S. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)* (2022), IEEE, pp. 842–859.

[53] LEHRE, F. . Hochschulen im visier von cyberkriminellen. https://www.forschung-und-lehre.de/management/hochschulen-im-visier-von-cyberkriminellen-5541, 2023. Accessed: 10-02-2024.

[54] LI, Y., STAFFORD, T. F., FULLER, B., AND ELLIS, S. Beyond compliance: Empowering employees' extra-role security behaviors in dynamic environments. In *AMCIS* (2017).

[55] MANSFIELD-DEVINE, S. Raising awareness: People are your last line of defence. *Computer Fraud & Security 2017*, 11 (2017), 10–14.

[56] MARIN, I. A., BURDA, P., ZANNONE, N., AND ALLODI, L. The influence of human factors on the intention to report phishing emails. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (2023), pp. 1–18.

[57] MENARD, P., BOTT, G. J., AND CROSSLER, R. E. User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems 34*, 4 (2017), 1203–1230.

[58] POSEY, C., ROBERTS, T., LOWRY, P. B., COURTNEY, J., AND BENNETT, B. Motivating the insider to protect organizational information assets: Evidence from protection motivation theory and rival explanations. In *The Dewald Roode workshop in information systems security* (2011), pp. 22–23.

[59] RAHIMI, S., AND KHATOONI, M. Saturation in qualitative research: An evolutionary concept analysis. *International Journal of Nursing Studies Advances 6* (2024), 100174.

[60] REEVES, A., CALIC, D., AND DELFABBRO, P. "generic and unusable" 1: Understanding employee perceptions of cybersecurity training and measuring advice fatigue. *Computers & Security 128* (2023), 103137.

[61] RENAUD, K., SEARLE, R., AND DUPUIS, M. Shame in cyber security: effective behavior modification tool or counterproductive foil? In *New Security Paradigms Workshop* (2021), pp. 70–87.

[62] RIZZONI, F., MAGALINI, S., CASAROLI, A., MARI, P., DIXON, M., AND COVENTRY, L. Phishing simulation exercise in a large hospital: A case study. *Digital Health 8* (2022), 20552076221081716.

[63] ROGERS, R. W. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology 91*, 1 (1975), 93–114.

[64] SASSE, M. A., HIELSCHER, J., FRIEDAUER, J., AND BUCKMANN, A. Rebooting it security awareness–how organisations can encourage and sustain secure behaviours. In *European Symposium on Research in Computer Security* (2022), Springer, pp. 248–265.

[65] SILIC, M., AND LOWRY, P. B. Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems 37*, 1 (2020), 129–161.

[66] SOLOMON, G., AND BROWN, I. The influence of organisational culture and information security culture on employee compliance behaviour. *Journal of Enterprise Information Management 34*, 4 (2021), 1203–1228.

[67] SON, J.-Y. Out of fear or desire? toward a better understanding of employees' motivation to follow is security policies. *Information & Management 48*, 7 (2011), 296–302.

[68] THOMAS, A., AND GUPTA, V. The role of motivation theories in knowledge sharing: an integrative theoretical reviews and future research agenda. *Kybernetes 51*, 1 (2022), 116–140.

[69] UCHICAGO. Latest phishing scams. https://security.uchicago.edu/phishing/latest/, 2024. Accessed: 10-02-2024.

[70] VANCE, A., SIPONEN, M., AND PAHNILA, S. Motivating is security compliance: Insights from habit and protection motivation theory. *Information & Management 49*, 3-4 (2012), 190–198.

[71] VERBISOFTWARE. Maxqda. https://www.maxqda.com/, 2022. Accessed: 10-02-2024.

[72] VOLKAMER, M., RENAUD, K., REINHEIMER, B., RACK, P., GHIGLIERI, M., MAYER, P., KUNZ, A., AND GERBER, N. Developing and evaluating a five minute phishing awareness video. In *Trust, Privacy and Security in Digital Business: 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5–6, 2018, Proceedings 15* (2018), Springer, pp. 119–134.

[73] WARKENTIN, M., JOHNSTON, A. C., AND SHROPSHIRE, J. The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems 20*, 3 (2011), 267–284.

[74] WEAVER, B. W., BRALY, A. M., AND LANE, D. M. Training users to identify phishing emails. *Journal of Educational Computing Research 59*, 6 (2021), 1169–1183.

[75] WEN, Z. A., LIN, Z., CHEN, R., AND ANDERSEN, E. What. hack: engaging anti-phishing training through a role-playing phishing simulation game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (2019), pp. 1–12.

[76] WIGFIELD, A., AND ECCLES, J. S. Expectancy–value theory of achievement motivation. *Contemporary educational psychology 25*, 1 (2000), 68–81.

[77] WIGFIELD, A., TONKS, S., AND KLAUDA, S. L. Expectancy-value theory. *Handbook of motivation at school 2* (2009), 55–74.

[78] WILKINSON, S. Focus group methodology: a review. *International journal of social research methodology 1*, 3 (1998), 181–203.

[79] WILLIAMS, E. J., HINDS, J., AND JOINSON, A. N. Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies 120* (2018), 1–13.

[80] WILLIAMS, P. Organisational culture: definitions, distinctions and functions. *Handbook of research methods for organisational culture* (2022), 5–22.

[81] YEOH, W., HUANG, H., LEE, W.-S., AL JAFARI, F., AND MANSSON, R. Simulated phishing attack and embedded training campaign. *Journal of Computer Information Systems 62*, 4 (2022), 802–821.

[82] ZHENG, S. Y., AND BECKER, I. Phishing to improve detection. In *Proceedings of the 2023 European Symposium on Usable Security* (2023), pp. 334–343.

[83] ZIMMERMANN, V., AND RENAUD, K. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies 131* (2019), 169–187.

A The core constructs of Expectancy-Value Theory

The core constructs of Expectancy-Value Theory as described in Eccles and Wigfield's work [25] are as follows:

- **Expectation of Success**: Individuals' beliefs regarding their potential effectiveness in executing tasks or resolving challenges [25].
- **Achievement-Related Choices and Performance**: The outcomes that individuals target when they choose to engage with an activity or perform a task, informed by their interpretation of expectation of success and perceived value of the specific task [25].
- **Subjective Task Value**: Individuals' assessment of a task's significance, utility, emotional resonance, and perceived cost [25].
- **Goal**: Cognitive representation of a future outcome that an individual is striving to achieve [24].
- **Self-schemata**: Cognitive generalizations about oneself, derived from past experiences and focused on self regarded importance [45].
- **Affective Reactions and Memories**: Individuals' emotional responses to specific tasks or scenarios, alongside the emotive memories derived from past experiences [76].
- **Perception of**: Individuals' interpretation and understanding of their previous experiences and socialization influences [76].
- **Interpretation of Experience**: The personal lens through which individuals perceive prior achievement-related events, influenced by a confluence of cultural, social, external feedback, and intrinsic cognitive and emotional factors [76].
- **Cultural Milieu**: A system of social roles, each with its associated responsibilities and obligations [77], this construct has been extended in our study to encompass "organizational culture."
- **Socializer**: Originally pertaining to parents, educators, and extended social circles in EVT [76], this construct has been adapted in our context to also include "colleagues and supervisors."
- **Person Characteristics**: The array of individual variances, encapsulating aspects such as abilities, personality dimensions, gender, age, and cultural origins [76].
- **Previous Achievement-Related Experiences**: Individuals' past experiences in activities or tasks that had a measurable outcome [25].

B The templates and focus group protocol

Introduction: Thank you for participating in this focus group discussion. This study is one part of the "anonymized" project, funded by "anonymized". This focus group aims to learn about employees' participation in and opinions on phishing awareness campaigns and reporting suspicious emails.

During the discussion, we will record audio and video and collect the paper materials. The collected data will only be used for this study. You have the right to access, rectify, and erase your data. Your participation in the project is voluntary; you can withdraw at any point without giving reasons. You may skip any task you do not wish to participate in for any reason, at any time, without explanation.

There are no right or wrong answers to the questions we prepared; also, we will not ask you questions about your passwords or whether you have encountered phishing attacks in the past. All your answers will be kept strictly confidential and will be anonymized, encrypted and only reviewed by the researchers of this project. Any data shown externally, for example in publications or presentations, will also be anonymized. Your data will be stored and processed only for the purpose of the study stated above for a period of 63 months on internal, on-premises servers.

The focus group will take approximately 90 minutes. Each participant will be compensated with a 40-euro voucher for participation. Do you have any questions so far? If you agree with the terms, please sign the consent form, and then we can start the recording and begin the focus group discussion. The focus group includes four main parts: warm-up activity,

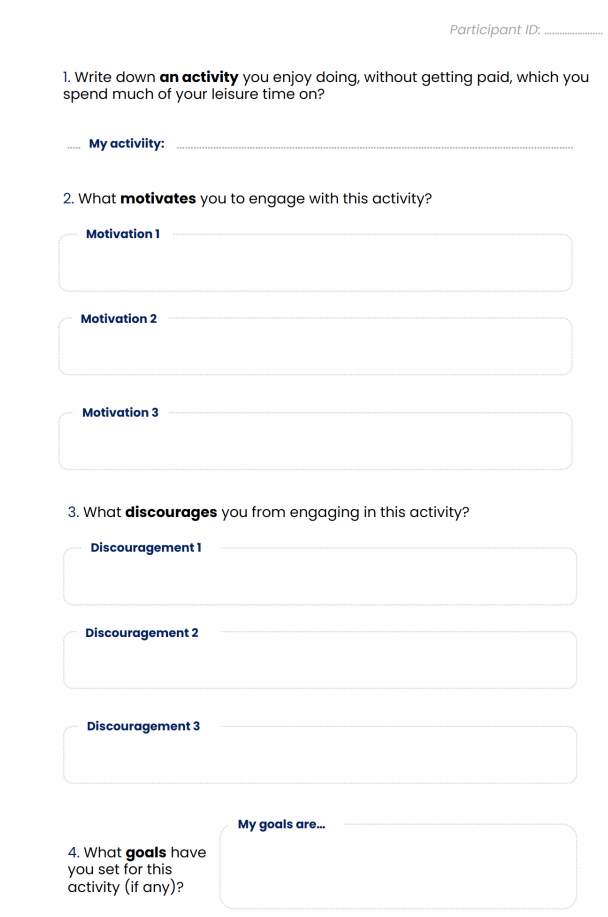

Figure 2: Template 1, what motivates and discourages you in a leisure activity.

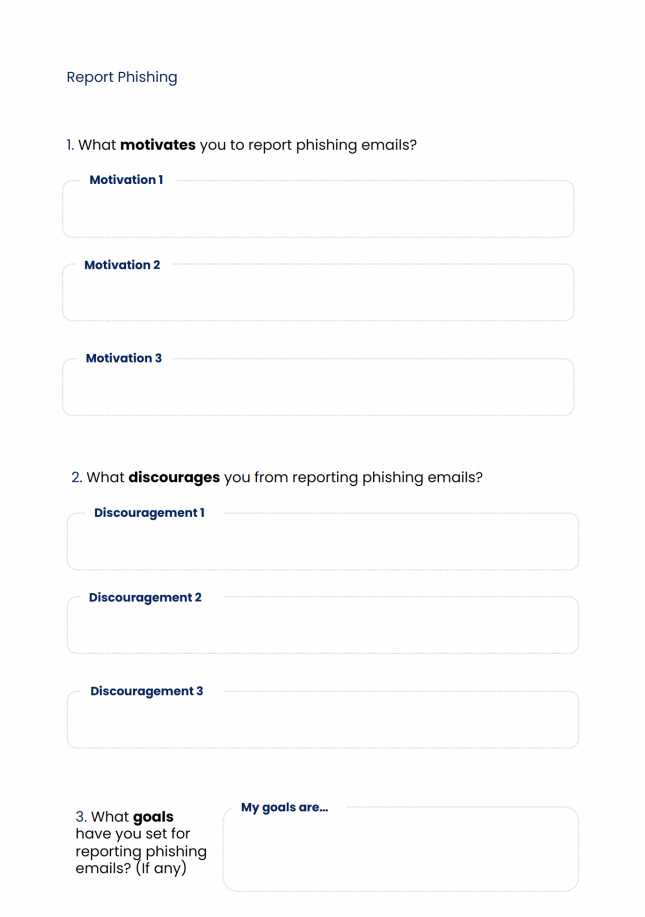

Figure 3: Template 2, what motivates and discourages you in reporting.

discussion, brainstorming and debriefing. Let's first have the warm-up activity.

Part 1: Warm-up activity (10 minutes):

Icebreaker: Now, you have 2 minutes to observe the items presented in the lab, try to spot one item that can be used to describe you today. We will share our thoughts after 2 minutes.

Explore motivational and discouraging factors for a leisure activity: Great, now we know each other. Let's move on to explore factors that motivate and discourage you from engaging in a leisure activity. You have 5 minutes to answer the questions on Template 1 (see Figure 2). After you finish, we will collect the paper.

Part 2: Group discussion (60 minutes):

Now, let's move on to the discussion session. Phishing attack is a type of social engineering attack where attackers send spoofed or deceptive messages to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the recipient's devices. Currently at our organization, we have several practices to raise employees' awareness of phishing attacks. First, the IT department sends simulated phishing emails to employees to raise awareness of potential phishing attacks. Second, our university has purchased online security courses from a service provider; you can access the learning platform via this link: "Anonymized". Third, the IT department distributes posters and sends emails to inform employees of online security courses. Some of you might have received these emails or saw the posters at the entrance to the administrative buildings.

Discuss phishing awareness campaigns:

1. What do you think of these three phishing campaigns offered by the IT team?
2. What are the benefits of participating in phishing campaigns?
3. What are the costs of participating in phishing campaigns?
4. Assuming that you know how to take the online security courses, what would discourage you from taking these courses?

5. Have you set any goals for yourself in terms of defending yourself from phishing attacks?
6. How confident are you in protecting yourself from phishing attacks?

Thank you for sharing these opinions with us. In our university, the IT department recommends that employees report phishing emails to report-a-phish@"anonymized"; the Outlook client now also has a report phishing emails button, so you can report with one click.

Now, you have five minutes to fill-in Template 2 (see Figure 3), "what motivates and discourages you from reporting suspicious emails"... Thank you and let's move on to **discuss reporting suspicious emails**:
1. The IT department suggests that we report phishing emails, what do you think of this suggestion?
2. How confident are you about identifying and reporting suspicious emails?
3. As a member of the organization, how do you see your role in reporting suspicious emails?
4. What are the benefits of reporting suspicious emails?
5. What are the costs of reporting suspicious emails?
6. What would discourage you from reporting phishing emails?

Part 3: Brainstorming (15 minutes): Assume that you are our university's new chief information security officer (CISO), and you learned that there are increasing phishing emails targeted at our university. What would you do to motivate employees to engage with these counter-phishing practices?

Part 4: Debriefing (5 minutes): Introduce the IT department recommendations of participating in phishing awareness campaigns and reporting suspicious emails.

C Coding scheme and exemplar quotes

C.1 Factors associated with phishing awareness campaigns

C.1.1 Motivating factors

Gaining phishing knowledge: Participants learned about the techniques and tricks of phishing attacks.

If you were participating in this awareness campaign, maybe get to know some new tricks and what is going on. Maybe there are new types of phishing. (P3)

Acquiring skills: Employees acquired skills in identifying whether the emails, links and website URLs are legitimate or not.

(Phishing campaigns)... train people to recognize what is phishing and prevent them from actually falling into one when it happens. (P22)

Enhancing phishing awareness: The phishing campaign raised employees' awareness of phishing attempts and made them more vigilant against potential attacks.

The good thing is if we make mistakes, they don't cost anything because they're internal mistakes. But they raise our awareness. (P26)

Cyber safety: Participants felt better prepared to protect themselves, their emails, and their workplace from phishing attacks.

It not only benefits you because you will protect your data and your e-mail accounts and so on; will also help the university as an institution to be better protected. (P9)

Personal development: Participants believed that the knowledge gained could benefit their daily life.

It's not only about fear of being attacked, you need to understand what's inside these technology tools... Everything related to cybersecurity is very fundamental now and, in the future, would become even more fundamental, like reading. (P29)

C.1.2 Discouraging factors

Perceived low value: Participants assumed that online phishing courses only provide very basic knowledge or use too complex terms for them to understand.

Don't give me a half hour course for two minutes' value. (P13)

Lack of interest: Negative impressions of the courses, such as "not interesting" and "too easy".

They look like really boring corporate mandated trainings and also the title "Anonymized", look at that and I'd be like oh no... (P17)

Secondary task: Participants mentioned that the phishing campaign was not relevant to their area of expertise or job position.

My role is more task oriented. So, I have to finish my tasks by the end of the day. If I take a course that's one hour long, that means I leave one hour later. (P24)

Lack of incentive: Participants considered lack of incentives, such as course credits, compensation, or praise from the team leader, as discouraging engagement with the awareness campaign.

What is my incentive to do an optional course here? (P24)

Time: Participants mentioned time as a constraint that discourages them from engaging in phishing campaigns.

Sometimes when you are busy, it's very hard to find an hour or so in a day to do them, and so it's quite a big constraint on that. I would say it's mainly time. (P9)

Interrupting workflow: Participating in awareness campaigns required people to switch away from the task at hand to phishing-related content.

The cost is the time spent, but also entering into the actual narrative and that type of discourse. Because you're doing something else and then you're switching to this. And you're like, OK, it's a completely different world, so it takes you away from your attention span. (P25)

Optimism bias: Participants mentioned that they believed they were less likely to fall for phishing than others.

I always had this thinking like, it won't happen to me because this is so stupid. (P14)

Overconfidence: Participants stated that they are very confident in their knowledge of the topic.

I should spend my time doing something else so it's like a prerequisite of this course like ... like 70 to 80% of course material they have already known. (P21)

Procrastination: Participants shared that procrastination resulted in delaying or "forgetting to" take the courses.

If there's no deadline, if there's no shock, I'll do it tomorrow, tomorrow, tomorrow. (P32)

Negative inference: Participants would become more worried about all the potential threats they might receive if they participated in awareness campaigns.

More negative inference ... we become a bit more scared about all these potential threats that we might receive. A little bit of stress in a sense that we need to be careful. (P30)

Fear of failing training: Previous bad experiences with awareness campaigns might evoke fear of failing the training.

The fear or the worry that if I failed the course, it would be tracked. Because I experienced that in the previous job. If you didn't get a certain grade, then you would be forced to retake it and retake it. (P8)

C.2 Factors associated with reporting

C.2.1 Motivating factors

Collaborating with the IT team: Participants considered reporting as a collaboration with the IT team. The IT team assists the employees in verifying the legitimacy of the emails, and employees assist the IT team in detecting the phishing attempts in real-time.

I think this is essential that we can report phishing to IT; and based on that they can have some statistics and see how the attacks are evolving. (P5)

Safeguarding the workplace: Participants regarded reporting as a measure to protect their workplace and colleagues.

Safeguard yourself, your institution, because I'm aware of phishing attacks that cause huge damages in the banking and insurance sector, in research departments overseas, and it's reputational damage that I would not like to be associated with. So protection for the whole institution and for me ultimately. (P13)

Expectation of mitigation: Participants expected that the organization would improve its spam filters and mitigate the attack promptly with the reported emails.

The main benefit of reporting is that the IT team could create more filters for phishing emails if they have more data (from reporting), making us safer (P27)

Recognition: Participants regarded the "congratulations" email they received from the IT team as a kind of recognition and extrinsic reward for their reporting.

And personally, it's always nice to have, like the congratulations, it's a nice accomplishment and you have the impression that you'd be helping the university community, so it's kind of rewarding. (P9)

Fear of consequences: Worries and fears related to not reporting prompt participants to report phishing attempts.

There're serious consequences if a phishing goes through, from a company perspective or on a personal level. (P13)

Sense of belonging: Participants expressed being part of the community prompts them to engage in reporting phishing.

We need to participate. We're all, we're all active users and it's not just IT who has to deal with it. (P32)

We are actors within the community. So, we are together. (P34)

Responsibility: Participants regarded reporting phishing as part of their job and shared the responsibility of reporting.

I see my role as a little more than this reporting, but also trying to reduce all the risk ... we have a duty. And you owe it to your colleagues as well as yourself. (P11)

Peer influence: Participants reported phishing emails because of the influence of their colleagues.

I used to ignore these emails, but then like one of my colleagues told me, it's better to report. So then I started doing it, yeah, but even I don't do it like every time, but most of the time I try to report them. (P21)

Easy to report: Participants mentioned that the positive user experience with the reporting process motivates them to report.

The reporting button is really easy, even if you're in doubt, you tend to click the button. (P13)

Protecting oneself: Participants considered reporting to benefit them in protecting personal accounts, avoiding financial losses, and safeguarding data.

If I never report anything, I can't expect it to just magically get better, so that's why I see a benefit for myself. (P26)

Phishing experience: Participants mentioned their experiences with phishing incidents as a driver for reporting.

I had this scam attack, and I felt bad about myself. I felt bad about trusting the others, so I wouldn't like someone, other people to feel the same way I felt once. (P4)

Empowerment: Participants considered reporting as an initiative against phishing attempts, giving them a sense of control and empowerment.

I had the initiative to defend against the phishing attack. And knowing that I can stop spreading this attack for other people and for my future self. That really helped me, like empowering. (P16)

Satisfaction: Participants expressed their sense of accomplishment/satisfaction for reporting suspicious emails.

I can relate to the sense of satisfaction. Once you've reported it, you feel like you played your role. You did a good job. (P11)

Enjoyment: Participants considered the reporting as a playful game or "nice welcome distraction" from work.

When you click to report phishing attempts, then you receive 'congratulations'. I'm happy and it's like a game. (P28)

Personal Value: Participants reported phishing attempts because it is the right thing to do or the suggestion is good.

It's a very good action to ask us to report suspicious emails. (P6)

Altruism: Participants wanted to help others and vulnerable groups, reducing their chances of being phished.

I want to help others avoid being deceived by phishing. (P15)

Pride: Participants mentioned pride stemming from their ability to consistently identify and avoid being phished.

I don't want to break my streak of always reporting the phishing attacks. I've not clicked on one socially engineered phishing e-mail, I'm quite proud of that. (P8)

C.2.2 Discouraging factors

Perceived low threat: If the participants regarded the incoming phishing emails as too obvious/low threat, they chose not to report.

If I consider the content of phishing emails so apparent, so explicit that everyone can find out that it's phishing, then I don't try to report it. (P16)

Negative outcomes: Assumed negative outcomes from reporting the email discouraged participants.

I feel like there's negative benefits for me reporting them because they don't seem to do anything with it and I just get more emails. So I would get the same amount of spam if I didn't report it. (P17)

Report too much: Participants expressed the concern that they reported too many suspicious emails and burdened the IT team.

It's already the second one I sent this week, so I said, what shall I do? (P28)

Worries of being judged: Participants expressed reservations about reporting suspicious emails due to worries of being judged by the IT team.

If I report Netflix or something as phishing, then they would think 'stupid woman'... This feeling unnerved me and discouraged me from reporting. (P34)

Privacy concerns: Participants expressed they were hesitant about reporting when they felt that it might divulge private information or create a false impression about their personal life.

I worry what they (the IT team) will think of me. So, I try to avoid informing them, because what are they doing with this information? (P28)

Switching between interfaces: Participants mentioned that even they intended to report suspicious emails, they tended to delete or ignore them when checking email on their smartphone.

I use the web client sometimes. I don't know if there is a report phishing on there, and I also don't know if it's on like the iPhone app. (P24)

Unclear procedures: Participants shared that unclear reporting procedures discouraged them from reporting suspicious emails.

I think you should report the suspicious emails, but it needs to be made clearer what suspicious e-mail is and how to properly report it. (P8)

Requiring too much effort: Participants who use Linux and Mac OS expressed that the reporting procedure requires too much effort.

It's too much effort for me, like not much effort, but it's not very easy. (P27)

Lack of feedback: Without follow-up or feedback on their reporting action, participants felt discouraged from reporting.

We don't know what the effectiveness of report-a-phish is. We don't know the numbers, so it would be really good to have a kind of feedback status. What has been done last year? What was the success rate? (P31)

Lack of communication: Participants felt discouraged due to not knowing whether their colleagues reported or not and the organization's status quo for reporting.

I report phishing emails regularly and religiously, but I'm thinking is everyone else doing the same as me, putting in the same effort as I am on reporting? It takes maybe 30 seconds of your time, butt I'm still very careful about it. (P25)

Low response efficacy: When they perceived no impactful results of their reporting, participants felt discouraged and even stop reporting.

If we feel it works, maybe we continue to report, but if it does not work so well, we will not report phishing again. (P1)

Habitual behavior: Participants shared that they often postponed or forgot to report because they reverted back to old habits of simply deleting emails.

Just going back to your old habits because this report phishing button for me is new. And in my other like personal e-mail, Gmail, what I do is delete. So, I might result in just deleting and then other times I might remember. (P11)

Laziness: Participants mention "laziness" as a self-reported reason for not reporting suspicious emails.

I'm able to report them, but sometimes I'm too lazy to report it. (P17)

Low self-efficacy: If they had too high doubts and were not confident about whether it was a phishing attempt or not, participants would not report.

For reporting, I'm not sure because sometimes I am not sure it indeed is a phish or not, so then sometimes, I just prefer to delete it and not to report. (P5)

Simulated or real attack: When simulated phishing tests are overused or not accompanied by a clear protocol, they result in reduced reporting intentions.

For me, every phishing email that I received was a simulated one. So, I didn't see the point of reporting that because

I knew that it was from IT. (P27)

Contextual factors: Overload at work, time pressure and stress when they received the email could discourage them from reporting.

Sometimes when I'm in a rush, I just delete. (P31)

D The demographic table

Table 2: Demographic table of focus groups.

Focus group	Participant	Job title	Field	Work experience (years)[a]
FG01	P1	Doctoral researcher	Computer Science	1
	P2	Lead software developer	IT	21
	P3	Doctoral researcher	Energy	4
	P4	Doctoral researcher	Robotics	12
	P5	Postdoctoral researcher	Security and cryptography	5
FG02	P6	Doctoral researcher	Psychology	7
	P7	Doctoral researcher	Psychology	2
	P8	Administrative assistant	Administration	2
	P9	Doctoral researcher	Political science and human rights	5
FG03	P10	Doctoral researcher	Neuroscience	5
	P11	Doctoral researcher	Social economics	5
	P12	Postdoctoral researcher	Engineering	8
	P13	Postdoctoral researcher	Digital health	23
	P14	Doctoral researcher	Political sciences	5
	P15	Doctoral researcher	Law	3
	P16	Doctoral researcher	Social sciences	1
FG04	P17	Doctoral researcher	Computer Science	5
	P18	Software developer	IT	20
	P19	Doctoral researcher	Computer Science	8
FG05	P20	Administrative assistant	Administration	25
	P21	Doctoral researcher	Supply chain management	2
	P22	Postdoctoral researcher	Security and cryptography	5
	P23	Doctoral researcher	Engineering	3
FG06	P24	Building project manager	Administration	13
	P25	Academic facilitator	Administration	26
	P26	Alumni relations	Administration	34
	P27	Software developer	IT & Admin	23
FG07	P28	Research facilitator	Administration	30
	P29	Data analyst	Administration	7
	P30	Research facilitator	Administration	21
	P31	Project manager	Administration	25
	P32	Research facilitator	Administration	27
	P33	Secretary	Administration	30
	P34	Administrative assistant	Administration	35

[a] We removed gender, age, and months working at the current organization to avoid re-identification. Work experience indicates the participants' total years of work experience, including previous jobs.