

USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

"I didn't know I would be this excited not to be scammed." Exploring Emotional and Behavioral Responses During Phishing Attacks

Raphael Weidhaas, *Aalto University;* Alexandra von Preuschen, *CISPA Helmholtz Center for Information Security;* Verena Distler, *Aalto University*

https://www.usenix.org/conference/soups2026/presentation/weidhaas

This paper is included in the Proceedings of the
Twenty-Second Symposium on Usable Privacy and Security.

August 24–26, 2026 • Hannover, Germany

ISBN 978-1-939133-59-5

Open access to the Proceedings of the
Twenty-Second Symposium on Usable Privacy and Security
is sponsored by USENIX.

"I didn't know I would be this excited not to be scammed." Exploring Emotional and Behavioral Responses During Phishing Attacks

Raphael Weidhaas
Aalto University

Alexandra von Preuschen
CISPA Helmholtz Center for Information Security

Verena Distler
Aalto University

Abstract

Humans remain vulnerable to phishing attacks, despite awareness, training, and technical measures. The role of emotions during phishing attacks is largely unexplored. Building on the appraisal theory of emotion, we investigated (1) which emotions are invoked during a phishing attack, (2) related cognitive appraisals, (3) behavioral responses during an attack, and (4) reflections about behavior throughout the attack. We conducted a qualitative study (N=41), simulating a workplace scenario during which a phishing attack occurs. We combined observation, interviews, and questionnaires. Emotions differed based on whether the phish was detected or not. The phish was frequently appraised as an interruption, invoking negative emotions. Not clicking on the phishing link was often appraised as a possible mistake, which may lead to reputational damage. Many participants reflected detecting the phish intuitively. This work contributes to an empirical understanding of emotions and behavior during phishing and provides research avenues and implications for how anti-phishing measures could benefit from emotion-aware solutions.

1 Introduction

In social engineering attacks, malicious actors use psychological manipulation techniques to compel their victims to perform specific actions [14, 47, 48]. A common attack vector is phishing, a frequent cause of data breaches [34]; it uses fraudulent emails impersonating trustworthy entities to obtain sensitive information [1, 47]. Phishing is a sociotechnical challenge that cannot be solved by technical measures alone, but requires humans as a last line of defense [22]. Automatic detection relies on blocklists of known phishing URLs [74], heuristics and page similarity detection [76], as well as AI [36]. But these methods cannot filter all phishing messages before they reach the user. Spear phishing messages, for instance, usually lack typical indicators and rely on building rapport with a potential victim [22].

Reactions to phishing emails have received considerable attention in the human-centered security community, for instance in the context of anti-phishing warnings [31, 50] or embedded user-training [43, 44, 63]. However, the critical moment during first exposure to a phishing email remains poorly understood from a psychological point of view. The emotional processes invoked during phishing situations can provide a compelling lens to understand the psychology of the attack process and associated behavioral responses. Despite their relevance for predicting behavior [17] and their impact on fast decision-making [35], the importance of emotions has so far been widely overlooked in cybersecurity research [70]. Thus, a research gap emerges around the causes and behavioral consequences of emotions during a phishing attack. Studying emotions helps us understand the reasons for both insecure and secure behaviors, and fosters enabling approaches for dealing with attacks [79].

We investigate the role of emotions through the appraisal theory of emotions [59], which describes the connection between emotions and behavior. We postulate the following research questions:

RQ1: Which emotions do participants report experiencing during a phishing attack?

RQ2: What cognitive appraisals (related to emotions) do participants report experiencing during a phishing attack?

RQ3: What behavioral responses do participants exhibit during a phishing attack?

RQ4: How do participants reflect on their (observed) behavioral responses during a phishing attack?

We conducted a qualitative study with 41 participants in a simulated office scenario. Participants were asked to complete a number of tasks "for an absent colleague", and were

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) 2026.
August 23–26, 2026, Hannover, Germany.

promised an incentive for accurate and timely completion. During this work, they received a simulated phishing email. Combining interviews, questionnaires, and observations, we gained deep insights into the emotional and behavioral processes during a phishing attack.

Our results illustrate the link between emotions and behavior. Annoyance and insecurity were reported by many participants who detected the phish. Different appraisals of the situation and the consequently invoked emotions played an important role in deciding to click or not. Flow, activity, unconcern, and involvement was mentioned by those who clicked the phishing link and provided data on the phishing website; surprise, worry, and confusion was associated with detection after clicking. Many participants doubted whether they detected the phish correctly. Some appraised that not clicking may be a mistake impacting others. This invoked anxiety, concern, and worry, and eventually led to clicking the link and providing data. Many reflected they first intuitively detected an oddity, which led to further inspection. Researching emotions helps us understand which factors in security-relevant situations lead to particular–possibly dangerous–behaviors through appraisal processes. This nuanced understanding cannot be gained when focusing solely on behavior or cognition.

This study is, to our best knowledge, the first study to apply a qualitative methodology grounded in the appraisal theory to explore emotions during a realistic phishing attack. This in-depth, in-situ insight into emotions and associated behavioral responses to a phishing attack stands out from previous studies, which for example observed emotions about hypothetical situations in questionnaires [2] or primarily focused on participants' actions in real-world settings without focusing on emotions [22]. Our study makes the following contributions:

- With findings rooted in the appraisal theory, we make a strong empirical contribution to a richer understanding of human factors underlying phishing susceptibility. Appraising a phishing email as the result of an earlier mistake, for instance, invoked an emotion process that led to clicking the phishing link and entering a password.
- Our work leads to actionable implications, such as transparent, periodic detection training that includes positive emotional reinforcement. Considering emotions in intervention design could help strengthen users' phishing detection skills.
- Our novel scenario-based methodology adds a valuable option to study phishing in a close-to real-life scenario with minimal deception.
- Our results include findings about emotional processes of participants who detected the phish. Understanding successful defense can reinforce secure behaviors [79].
- We identified a behavior that did not receive much attention in research yet: Participants who did not click on the link, but also did not suspect phishing. They may click later - a looming risk that needs further investigation.

2 Related Work

2.1 Phishing Experiences

Phishing is the most prevalent cyberattack [34] and typically manifests through deceptive emails, websites, text messages, or phone calls. Designed to create urgency, fear, or curiosity, the messages compel immediate action from victims [18]. Inspired by conceptual frameworks of Abroshan et al. [3] and Zhuo et al. [78], we define email phishing from a user's perspective as a before-during-after-attack process (Figure 1).

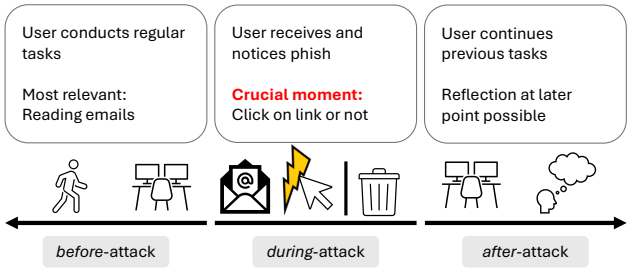


Figure 1: Before-during-after phishing process from a user's perspective.

The *before*-attack period encompasses all activities preceeding the arrival of a phishing email; most relevant are tasks in an environment related to phishing (e.g., answering emails, browsing the web). The *during*-attack period begins when a user notices the new email and includes the most crucial actions: reading the email, clicking the malicious link (and providing data), or detecting the phish. The *after*-attack period starts when a user resumes their task or starts another.

Embedded phishing training assumes individuals falling for a simulated phishing email are particularly receptive to awareness training in the moment of clicking, a situation referred to as a "teachable moment" [68]. While some studies show promising openness for learning [41,42], other research emphasizes that this approach is only effective when individuals are sufficiently motivated for the training [12,30,68]. The experience of failure caused by the simulated phish may be counterproductive [68].

Experiences with phishing attacks are likely connected to emotions, which, in turn, are linked to future security behavior [69]. Given the limited exploration of emotions during phishing attack interactions, there is a need to research the role of emotions in the during-attack period.

2.2 Emotions and Appraisal

This work is grounded in the component process definition of emotions, an appraisal theory by Scherer [59]. The theory links emotion with cognition and emphasizes emotions as a driving force for behavior. Emotions are distinct from related concepts like feeling, affect, or mood, and include five

components, which can be measured individually: appraisal, bodily symptoms, preparation for action, behavioral intention, and subjective feeling (Tables 3 and 4 in Appendix provide details). Scherer's theory is widely accepted and various tools to measure emotion components are available.

The emotion process [59] begins with stimuli (events) affecting the organism, such as external events (e.g., arriving email), own behavior (e.g., reading), or internal phenomena (e.g., memories). Emotions are then produced through a sequence of appraisal checks, a cognitive evaluation of the stimuli. Possible consequences in respect to the current needs and goals are evaluated. The emotion prepares the appropriate response behavior, which must correspond with the result of the appraisal check – the possible implications of the event. Since stimuli can change rapidly, the appraisal must re-evaluate a situation and change as well (reappraisal). Emotions can transform during an event, consequently current behavior may be interrupted and change.

Scherer's [59] definition illustrates how emotions are intertwined with behavior. The influence of emotion on behavior has been studied in behavioral sciences [64, 65], economics [11], and environmental sciences [75].

2.3 Emotions and Cybersecurity

2.3.1 Emotions in Cybersecurity Research

Human-centered security research has only recently started to consider emotions. In their literature review, von Preuschen et al. [70] identified 23 papers examining emotions in cybersecurity. They called for more qualitative studies to assess incidental emotions and behavior, while considering the complexity of both cybersecurity and emotions.

Quantitative research in the field has been criticized for often oversimplifying emotions [70]. One study [13], for instance, developed a short questionnaire for measuring all five emotion components (cf. [59]) related to cybersecurity. Other work did not provide any definitions of emotion [28], or measured affect but called it emotion [37, 55].

Related qualitative research is still scarce [70]. Renaud et al. [54] utilized an artistic method to explore emotions around cybersecurity without prompting them. Most respondents felt negatively towards the topic. Another study aimed to draw a holistic picture of emotions around cybersecurity via in-depth interviews [69]. The authors presented diverse, at times conflicting emotions, and illustrated their relevant consequences.

2.3.2 Emotions to Understand Behavior During Phishing

The aforementioned literature review [70] listed only a single paper examining emotions related to phishing attacks. The work [2] examined the influence of fear, anxiety, and stress regarding the COVID-19 pandemic on phishing susceptibility and found that external anxiety and stress influenced the success of phishing. Some other studies did not study emotions primarily, but they were part of their findings. Distler [22] included a question about feelings in an interview after simulated spear-phishing. Others interviewed users about privacy-related panic situations and discovered phishing attempts as a relevant trigger of panic, even if unsuccessful [4]. House & Raja [33] observed fear arousal and self-confidence of individuals presented with phishing attacks. Another study observed regrets around cybersecurity and found phishing to be related to regret and learning [53]. None of these studies explored emotions elicited during a phishing attack, which are likely to influence behavioral reactions to the phish.

3 Methodology

3.1 Research Design Overview

Recreating a natural setting to examine phishing attacks is challenging. We had to balance ethical and practical aspects, while maintaining sufficient emotional realism to address our research questions [23, 24]. Phishing usually interrupts a user, as it typically occurs while one is focused on an unrelated primary task (cf. Figure 1). We recreated a common office setting to observe the emotional reaction to an unexpected phishing attack in-situ. We asked participants to imagine a scenario where they were working at our university; we gave them ten tasks and promised a bonus upon completing all of them. While working, participants received a simulated, risk-free phishing email. We were interested in the diversity of emotions *during* a phishing attack, independent of behavioral reactions to the phish. After the task session, we conducted interviews to understand participants' emotions during the attack. Figure 2 presents an overview of the procedure. The study protocol can be found in Supplementary Material A.

3.2 Recruitment and Participants

We targeted students and staff of Aalto University. Participants were recruited via posters, social media, emails, and snowballing. Invitation postings (see Appendix, Figure 7) included a link to a registration questionnaire assessing demographics, ability to work with common office software (e.g., Microsoft Outlook), current field of work or study, and the Self-Rated Emotional Intelligence Scale [8], which indicates how well one is able to reflect their own emotions (inspired by [69]). To avoid priming, we did not mention phishing during recruitment. 41 participants took part in the study (20 female, 20 male, 1 preferred not to say; mean age: 27.68 years, SD: 5.14). The sample consisted of 22 students and 19 academic staff members from diverse disciplines. All were familiar with office software. The mean Emotional Intelligence score was 3.44 (Median: 4, SD: 0.45). No participants were excluded. The study was conducted in English in summer 2025.

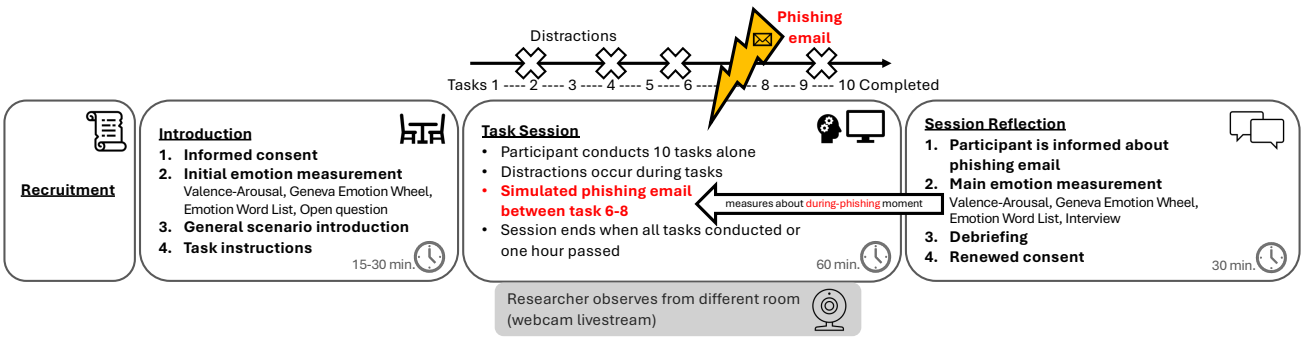


Figure 2: Summary of methodology procedure. Note that the main emotion measurement (questionnaires and interviews) focused on the during-phishing moment, which participants encountered in the task session.

3.3 Ethics Statement

The study was approved by Aalto University's ethics board. Participants received a privacy notice, gave informed consent, and related questions were answered. To ensure genuine emotional reactions during the phishing situation, we could not disclose the full study protocol to participants initially. We invited to a study about "Emotions in Cybersecurity", but did not mention phishing. Invitation postings advised people sensitive to the topics to avoid participating (see Appendix, Figure 7). We believe the benefit of understanding emotions and their impact on behavior during phishing outweighs the risks of participants losing trust in science or feeling deceived. To avoid negative consequences due to participation, we followed APA guidelines [5] and debriefed participants about the purpose of the phishing email. Information material about phishing prevention was offered in addition. Consent was renewed at the end of each session. Participants had the right to withdraw from the study at any point, with all collected data being deleted. We collected minimal data. All data was pseudonymized during analysis and all sensitive data, direct, and indirect identifiers were deleted. The phishing emails and -website were risk-free and did not save any input. Email communication was deleted after each session. Participation took around two hours. Participants received a 30€ restaurant voucher, plus a 10€ bonus after debriefing. The bonus was promised as an incentive, but was given to every participant, independent of performance, to ensure equal compensation.

3.4 Study Setting & Procedure

3.4.1 Laboratory Environment and Pretests

We set up a room resembling offices in Aalto University (see Appendix, Figure 9), including a computer running the university-wide operating system and software. Participants conducted the tasks alone, a tripod-mounted webcam (Logitech C925e) connected to a laptop was used to observe the participants' screen from another room. We recorded interview audio (Zoom H5 recorder).

Participants used their university accounts and email inboxes. This provided the advantage of a familiar digital environment and a more realistic risk representation. Since the study was conducted during summer holidays, we did not expect much communication external to the study. No participant received other emails than ours during any session. We conducted four pretests, which resulted in minor changes to the order of events and refined interview questions.

3.4.2 Informed Consent & Initial Emotion Measurement

After introduction and informed consent, we conducted the first measurement to control for emotions invoked by the laboratory setting and possible outliers. We used valence-arousal [57], the Geneva Emotion Wheel (GEW) [60,61], and an Emotion Word List [69].

3.4.3 General Scenario Introduction & Context

We then asked participants to situate themselves in a scenario: They started a summer job as an event coordinator at Aalto University, representing a colleague on holidays. As part of the "anniversary team", they helped to organize a gala for the university's anniversary celebrations. The colleague on leave left a list with ten tasks that should be completed soon. As their supervisor was stressed about the nearing event, they promised a 10€ bonus if all tasks were completed successfully in this session. Scenario and tasks were designed with the help of an event coordinator from Aalto University. The familiar campus setting allows to recreate a context as it occurs in daily life, as recommended by Greenaway et al. [32].

3.4.4 Task Instructions

Acting as a colleague, the researcher walked participants through the tasks and made sure they were familiar with the software needed. Two example tasks: (1) "Write arrival instructions to [event location]. Include public transport and parking. Send result to event team.", (2) "Create two Zoom-meeting links and send them to speakers, including a short

greeting." (full list in Appendix, Table 5). Participants were encouraged to call for help in case of problems, this would not impact the bonus. We emphasized that using the email client was essential for completing the session successfully, since colleagues may send further requests to tasks, as in real work environments.

Under the pretext that new employees need to set up user accounts, we briefly discussed passwords with participants to prevent suspicions about the study objectives ("emotions in cybersecurity"). Next, participants began to work alone. The researcher left the room and started the observation.

3.4.5 Task Session

Participants were asked to complete ten tasks in the given order within one hour. Task-related and irrelevant emails were introduced as realistic distractions (see Appendix, Figure 12). The session ended after all tasks were completed or one hour passed. All interactions were controlled by the observing researcher, utilizing the livestream of the participants screen.

3.4.6 Phishing Attack

Between task six to eight (mean: after 44 minutes, SD: 4.75), participants received **one** phishing email (see Appendix, Figure 10). We designed pretexts related to software used during the session: Zoom and Webropol. A target-related pretext can increase click-rates [29], which is beneficial in this setup. As it is public information that Aalto University uses Zoom and Webropol (e.g., guides on website), it is plausible that attackers could exploit this information.

To guarantee task-related pretexts, we designed two phishing emails in case one of the tasks was not completed (see Appendix, Figure 8 for the decision process). The Webropol email was our primary choice, since providers blocked our mock addresses containing "Zoom" (or variations) more often. It is unlikely that one would receive multiple phishing emails in one hour, so each participant received only one phishing email.

Both pretexts mimicked official emails. They included several red flags, allowing participants to detect the phish. The emails contained links to mock phishing websites, which asked for username and password. Upon clicking "submit", the webpage displayed a "success"-message. Emails and website can be found in the Appendix, Figures 10 and 11.

3.4.7 Information about Phishing Email

Participants were informed about the phish regardless of their reaction to it. We then showed them an image of the phishing email to help reflect on their experienced emotions [51] *in the moment of encountering the phishing email during the task session*. To emphasize that the interview focused on the *during*-attack period, we also explained the phishing process using Figure 1.

3.4.8 Main Data Collection

We measured four of Scherer's five emotion components [59] (cf. Section 2.2): subjective feeling, appraisal, and preparation for action via questionnaires and interview; and behavior/behavioral intention via observation and interview.

Following guidelines [27,51,58,59], we used multiple measurement instruments with increasing level of detail to ensure participants were comfortable reflecting on their emotions. We began with three questionnaires assessing subjective feeling: (1) Self-Assessment Manikin (Valence-Arousal) [9], (2) Geneva Emotion Wheel (GEW) [60, 61], and (3) Emotion Word List [69] (see Supplementary Material B). Our results focus on the List, as it is most detailed and overlaps with the GEW (see Supplementary Material E and F).

This was followed by an interview, in which we discussed the questionnaires and inquired in depth into emotion components [59]. For example, we asked how appraisal of the phishing situation shaped feelings or how participants formed their behavioral intentions (questions based on [16, 27, 66]; full interview protocol in Supplementary Material A.)

Emotion measurements always include tradeoffs [52]. We decided to use a recall-based method as other options would have been invasive. Asking participants about their emotions immediately once they received the email would have interrupted the simulation and invoked unrelated emotions. The use of sensors to measure physical arousal may have primed participants to expect strong emotions. We focused on subjective experience instead of sensor data to assess complex constellations, as prior research displayed that emotions in cybersecurity go beyond basic emotions that can be captured by physical indicators [69]. We recognize that retrospective accounts can introduce recall bias. To minimize this, we followed best practices [52] to enhance recall reliability: emotions were measured max. 20 minutes after encountering the phish; we provided an image of the phishing email during the interview; and we combined multiple measurement instruments.

3.5 Data Analysis and Methodological Integrity

Table 1 provides an overview of used data sources. We transcribed all interviews. Microsoft Excel was used for quantitative analysis. We conducted Kuckartz' Thematic Qualitative Text Analysis [38] (p. 89ff), using MAXQDA 2024 [39]. The term "code" refers to the categories built during analysis; the coding unit was defined as a statement that makes sense on its own in relation to the sub-code. Supplementary Material C describes our analysis in detail.

We began categorizing the data in general top-codes based on research questions and then created sub-codes inductively based on top-codes, memos, and summaries. Instead of reliability scores, we used consensual coding as recommended by Kuckartz [38] (p. 95): After a first co-coding session with

Table 1: Data sources used to answer each research question.

Research Question	Data Source
RQ1: *Which emotions do participants report experiencing during a phishing attack?*	GEW and Emotion Word List; Qualitative analysis of interviews
RQ2: *What cognitive appraisals (related to emotions) do participants report experiencing during a phishing attack?*	Qualitative analysis of interviews
RQ3: *What behavioral responses do participants exhibit during a phishing attack?*	Qualitative analysis of observation notes and interviews
RQ4: *How do participants reflect on their (observed) behavioral responses during a phishing attack?*	Qualitative analysis of observation notes and interviews

three co-authors, we organized sub-codes into relevant top-dimensions and edited unclear codes. The new system was tested via another co-coding session; we edited unclear codes until we reached consensus. The elaborate system was used in the second coding process (Codebook in Supplementary Material D). We then created a thematic matrix and summarized the cases for each participant's top categories. The summaries were used for category-based analysis, as reported in the results. We used a generalized system for quantifiers (e.g., some, many), found in Supplementary Material H. The frequencies of codes (number of participants) are reported in brackets.

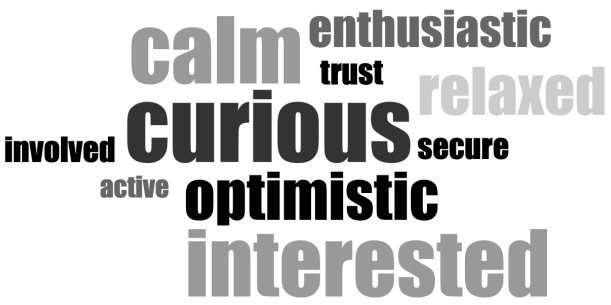


Figure 3: The top ten choices of the Emotion Word List by all participants (N=41) **before** the task session. We conducted this measurement to control for emotions invoked by the study setup. We did not detect any outliers. Word sizes represent choice frequency. Participants could choose multiple emotions. Details in Appendix, Table 6.

3.6 Limitations

This is a qualitative and explorative study, our findings are not generalizable to the general population or all phishing contexts. Qualitative content analysis does not aim to generalize; it aims to gain a deep understanding of and interpret the underlying material [38]. With our methodology, we exemplify **one** possible situation, and seek rich insights into it. Educational background and the university-related scenario setting might have impacted the results.

There was no way to control for how many people would click and provide data. With a click-rate of 29%, our results are higher than those in current reports from simulated phishing solution vendors (20%) [6].

Finally, no matter how well designed, some aspects of reality cannot be simulated: more social interaction or unplanned breaks may occur in real-life scenarios. Our participants had one hour to conduct their tasks; while urgency can be part of a real workday, users might consider interacting with an email later.

4 Results

4.1 Participant Groups

We categorized participants in four groups based on interactions with the phishing email:

- **Detected as phishing (n=22):** "detectors" (D)
- **Did not click but did not detect as phishing (n=7):** "non-detectors" (N)
- **Clicked phishing link (n=8):** "clickers" (C)
- **Provided data on phishing website (n=4):** "phished (participants)" (P)

For a detailed report about behavioral responses (RQ3), see Section 4.6. We provide group abbreviations (D, N, C, P) with participant quotes and refer to "all" (N=41) if a code was observed frequently among all groups. We do not refer to groups in Sections 4.2 and 4.3.

4.2 Participant Immersion

Participants reflected the task session as if it had been a real-life event and mentioned how it resembled their own work routines or previous jobs. Due to this immersion, they did not think about the advertised cybersecurity focus, as 121P illustrated: *"As a coordinator at an institution, I didn't feel like [I would receive] some kind of cyberattack. I feel, and I was also feeling, trust and confidence."*

4.3 Emotions Before Task Session

Figure 3 presents an overview of the emotion words selected **before** the task session. Participants generally experienced positive emotions. In the open question, all participants answered that they had a positive attitude towards taking part in a study. GEW results can be found in Supplementary Material E.

4.4 Emotions Experienced During Phishing Attack (RQ1)

To address RQ1, participants were asked to reflect the emotional state they experienced in the during-phishing period (cf. Figure 1). We present the most-selected emotion words from the Emotion Word List in Figure 4. Details in Appendix, Table 6. GEW Results in Supplementary Material F.

> **Key Results – RQ1 – Emotions During Phishing:** Figure 4 illustrates how the reported emotions differ based on how participants interacted with the phishing email. Especially **non-detectors** (4b) and **phished participants** (4d) reported mostly positive emotions. Despite similar behavior (clicking on the phishing link), **clickers** (4c) exhibited a different palette and reported surprise and worry. **Detectors** (4a) stand out as the reported emotions are mostly negative.

4.5 Cognitive Appraisals During Phishing Attack (RQ2)

Figure 5 presents a simplified overview of all cognitive appraisals. Detailed descriptions below.

4.5.1 Appraisal of Email Arrival

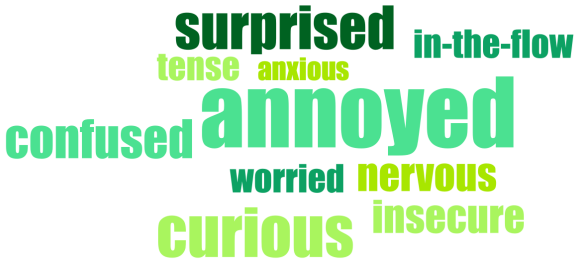
All: Many (16) initially appraised the arrival of the email as a positive event, e.g., task confirmation. Some (9) thought of an additional task that needs to be executed. This usually invoked curiosity, interest, or surprise.
Detectors: For about half (13), skimming the email teaser or content led to a reappraisal of the situation as an interruption of current flow of work. This usually invoked annoyance. Some (7) immediately appraised the situation as a phishing situation, in which they need to be cautious and act deliberately.
Non-detectors: A few (3) also appraised the arrival of the email as an interruption and disturbance, invoking negative feelings. 104N illustrates: *"Then you get an email and [...] it's just annoying questionnaires [...], flooding my inbox for no reason. Thanks for that."*.
Clickers: Almost all clickers (7), appraised the situation as an interruption. The invoked emotions are diverse, spanning from active (127C), to confused (105C), to anxious (130C).
Phished: Half (2) appraised the arrival as an interruption that needs to be eliminated to avoid disrupting their current flow. 103P stated: *"That intervenes with the task that I'm doing right now so it takes away my attention [...] you're in the flow and that annoys you somewhat. But then it's nothing that big. It doesn't take lots of time."*

4.5.2 Appraisal of Email Content

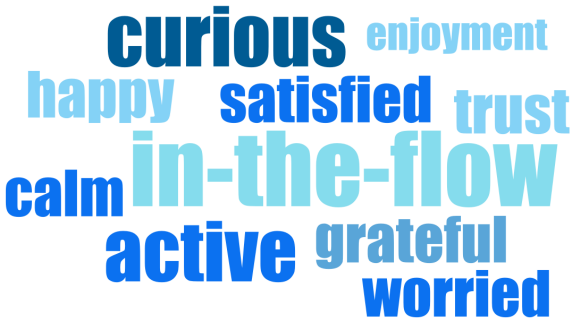
All: Some (13) appraised the email content relating to a supposedly completed task.
Detectors: Many (8) exhibited cognitive dissonance: they were cautious about the email (due to detection or vigilance) but on the other hand thought, clicking might be necessary to complete a task. This created the feeling of ambivalence.
Non-detectors: Some (3) appraised the content of the email as legitimate. For three, it posed a challenge, expecting additional work for a supposedly completed task. This appraisal was related to frustration and anger. Cognitive dissonance was also observed here: about half non-detectors (4) were convinced they already completed the task (questionnaire or Zoom), and the content of the email did not make sense in relation to the task. This invoked anger and frustration, as for 104N: *"I know that I sent it. So, I don't know what else to do! It was a 'what-the-hell'-moment."*
Clickers: Also appraised as legitimate by most (5), for example 107C: *"I remember looking at the preview and it's saying, you're almost done with publishing your survey. And it made sense [...]."*. Similar to non-detectors, some (2) appraised the situation as challenging and mentioned frustration and annoyance. Most participants in this group (5) experienced cognitive dissonance because of the vague email content. They reported confusion, ambivalence, and indifference.
Phished: Three appraised the content as legitimate. Half (2) of the group also appraised the situation as challenging and problematic. This invoked negative emotions such as frustration and annoyance.

4.5.3 Appraisal of Call to Action in Email

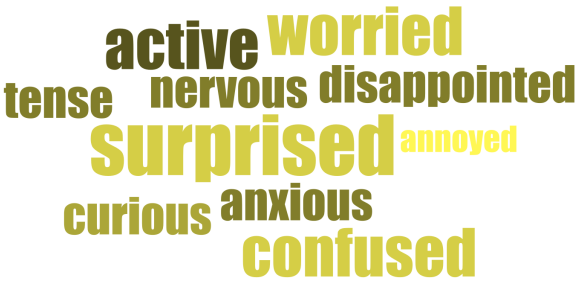
Detectors: Some (5) began to reappraise the situation as problematic as they became suspicious about possible phishing. Many (9) still exhibited cognitive dissonance and imagined the consequences of a potential detection error. This invoked feelings of uncertainty and insecurity and made a few (4) worry about a possible impact on their reputation at work; to illustrate *"What if my judgment is wrong? Then it would cause my reputation, my work and performance to be questioned."* (117D). Finally, some (5) were convinced that the email is a phish and reappraised the situation as problematic.
Non-detectors: No further reports since they decided not to take any action from this point.



(a) Detected as phishing, n=22



(b) Did not click but did not detect as phishing, n=7



(c) Clicked phishing link, n=8



(d) Provided data on phishing website, n=4

Figure 4: The top ten choices of the Emotion Word List (split by participant groups), addressing RQ1. Word sizes represent choice frequency. Participants could choose multiple emotions. Details in Appendix, Table 6.

Clickers: Half (4) appraised the call to action as a result of a previous mistake they made. This invoked emotions like anxiety, concern, insecurity, nervousness, and tenseness. This led some (3) to create a mental scenario of fictional consequences of their mistake. 132C mentioned: *"What should I do? [...] take off a box that says anyone can join? Make this open invite? But you have to be secure, it's an interview with a guest, it cannot just be a public meeting."* Some (3) then suspected a phish and reappraised this as problematic. Three experienced cognitive dissonance and imagined the consequences of an erroneous detection. Two were also worried about their work reputation in this regard. Uncertainty and insecurity was reported. Ultimately, half (4) believed the email was legitimate and likely result of a mistake.

Phished: Half (2) were immediately convinced they made a mistake that resulted in the email, which invoked anxiety, insecurity, and nervousness. Two participants imagined a third person was waiting for them, which created urgency. This invoked worry, guilt, concern, and tenseness. 121P illustrated: *"The colleague who left has already [...] scheduled this Zoom meeting. As I was acting on behalf of him, I thought I should allow this guy [to enter the Zoom meeting] without going through all the details in the email. [...] I immediately had some kind of guilt that he was already waiting for long."*.

4.5.4 Appraisal of Clicking and Phishing-Website

Clickers: Once the phishing website opened, most (6) appraised the situation as problematic, realizing they clicked on a phishing link. This invoked shame, guilt, disappointment, and helplessness, as for 127C: *"And after clicking the link, I was a bit frustrated. Like, why did I click it? Why didn't I just check the sender? And I did feel a little bit helpless because I didn't know what to do next. And disappointed and guilty."* Some clickers (3) also considered possible damage from clicking, reporting worry, fear, and anxiety.
Phished: Half of the group (2) appraised the situation of clicking and providing data as an accomplishment. They appraised self-efficacy after solving a task or fixing a mistake, which evoked feelings of pride, relief, and satisfaction.

4.5.5 Appraisal of Phish Detection

Detectors: All recognized the phish based on the "red flags" in the email (see Appendix, Figure 10). After detection, about half (12) appraised that they are able to deal with the situation. This self-efficacy invoked pride, confidence, and relief. 118D was excited about the detection: *"I didn't know I would be this excited not to be scammed - it's like it's vindictive!"*

Next, some (5) appraised the situation as amusing - either

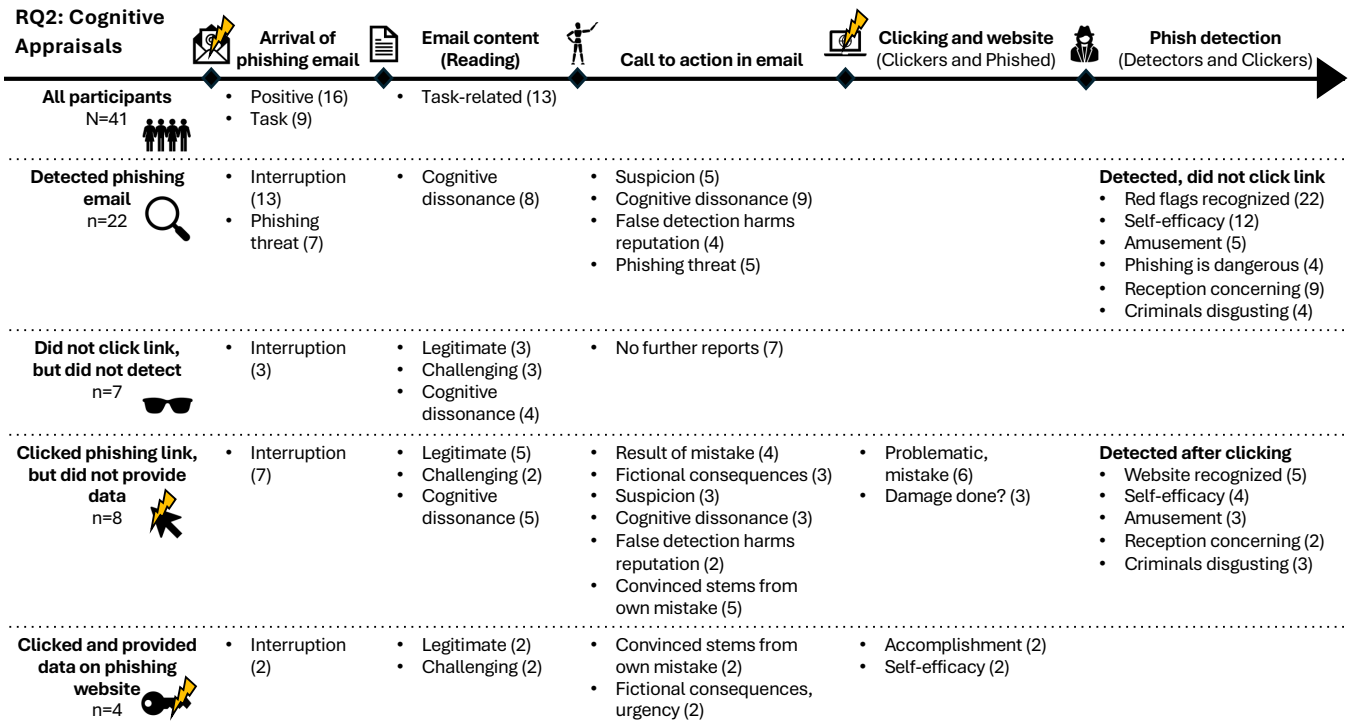


Figure 5: A simplified overview of all cognitive appraisals in chronological order, addressing RQ2. Code frequencies in brackets. Columns refer to respective subsections, rows to participant groups. Bullet-points represent codes.

based on the content of the phish or website, or because of the peculiarity of the situation itself. Conversely, a few (4) reappraised the situation as dangerous. Many (9) became concerned about receiving a phishing email; e.g., fearing data leaks. Four exhibited hate and disgust towards cybercriminals. **Clickers:** Most (5) detected the website as phishing. Akin to detectors, half (4) appraised self-efficacy and reported similar feelings, three were amused, two became concerned about receiving a phish, some (3) were disgusted by criminals.

> **Key Results – RQ2 – Cognitive Appraisals:**
> **Detectors** appraised email as interruption, which raised suspicions; experienced self-efficacy. **Non-detectors** appraised phish as legitimate interruption, but currently unimportant. **Clickers** appraised email as result of own mistakes, and behavior as problematic after clicking. **Phished participants** appraised providing data as an accomplishment (corrected own mistake); reported self-efficacy.

4.6 Behavioral Responses During Phishing Attack (RQ3)

Table 2 illustrates the diverse sequences of observed behavior in every group. Detectors exhibited various inspection strategies – so did clickers, but only after the phishing website opened. Non-detectors did not show further interaction after reading, and phished participants displayed the behavior exactly as requested by our phishing email.

> **Key Results – RQ3 – Behavioral Responses:**
> While **detectors** inspected the link, sender, and/or sought further clarification, **non-detectors** showed little interaction with the phish. **Clickers** double-checked the sender or website after clicking. **Phished participants** exhibit the most straightforward behavior, complying with the email.

4.7 Reflection on Behavior During Phishing Attack (RQ4)

Figure 6 presents a simplified overview of the reflections. Detailed descriptions below.

4.7.1 Reflection of Detection

Detectors: Some (7) reflected they initially detected the email based on an intuitive gut-feeling, which led to a more conscious inspection. Exemplary, 123D: *"[...] somehow it felt wrong, something strange, uncanny about this email."* A conscious, systematic inspection was mentioned by the majority of detectors (16).

Clickers: Three noted they detected the website intuitively.

Table 2: All observed behaviors in the during-phishing period and their frequencies (split by participant groups), addressing RQ3. Does not include observations before arrival of the phishing email.

Behavior/Group	Detectors	Non-Detectors	Clickers	Phished	Total
Recognized and opened email during session	22	7	8	4	**41**
Opens phishing email immediately at arrival	7	0	2	1	**10**
Reads email and continues (no other observable reaction)	8	7	0	0	**15**
Physically freezing for a moment	5	0	1	0	**6**
Inspects link and/or email-address	9	0	1	0	**10**
Checks related service (e.g., Zoom) for clarification	3	0	0	0	**3**
Writes email to supervisor, asking for clarification	2	0	0	0	**2**
Checks task list for clarification	2	0	1	0	**3**
Clicks on phishing link without further inspection	0	0	7	4	**11**
Inspects link and/or email-address after clicking	0	0	3	0	**3**
Reports email as phishing and/or blocks sender	4	0	2	0	**6**
Provides username and password on phishing website	0	0	0	4	**4**
Inspects phishing website	0	0	2	0	**2**
Marks phishing email as unread	2	0	0	0	**2**
Answers to phishing email: "task done"	0	0	0	2	**2**

4.7.2 Reflection of Non-Detection

Non-detectors: All (7) believed the email was legitimate and only learned it was a phish in the interview. Almost all (6) believed that the problem presented in the email was not urgent and could be solved later. Some (3) forgot about the email after deciding not to interact with it. Six admitted that they would have clicked the link later.
Clickers: Almost all (7) considered the email legitimate. Half (4) thought the email was result of a mistake or unfinished task, so they wanted to correct it. A few (2) mentioned, they did not fully read the email before clicking. Two reflected that they would have provided data later.
Phished: All (4) believed the email was legitimate, resulting from a mistake which has to be corrected. Two reflected they were deeply in the flow when the email arrived, and just did whatever was asked. Those two noted they did not fully read the email before clicking. The others (2) read the email, but were convinced they had to urgently click on the link to correct their mistake.

4.7.3 Reflections of Behavior in During-Period

Detectors: A few (4) decided to tackle uncertainty about the email by simply not reacting to it. We observed different forms of externalization (among all groups). Three were sure they completed the task and did not have to bother, two believed it was safer to wait for arising problems instead of clicking on a possible phishing link. A few (2) detectors were disappointed about their inappropriate reaction, e.g., not reporting.
Non-detectors: About half (4) chose inaction, one also preferred waiting for problems rather than clicking; some (3) externalized the responsibility and noted that obstacles were not their problem after completing the task, 101N illustrated: *"I did not care about the email. After all I was just thinking that it's from some Zoom person, so I don't have to mind about that, as if I had no other tasks to do."*
Clickers: A few (2) reflected they clicked because they were not familiar with the related tool (i.e., Webropol or Zoom). Some (3) were ashamed about clicking the link or not being fully concentrated.
Phished: No further reflections.

> **Key Results – RQ4 – Reflections on Behavior:** **Detection** often began with intuition. **Non-detectors** thought the email was not urgent but would click later. **Clickers** wanted to correct a mistake. **Phished participants** believed their mistake affected others and warranted urgent action, or they simply complied. Participants in **all groups** externalized their actions.

5 Discussion

5.1 The Impact of Emotions on Behavior During Phishing

Our findings demonstrate how Scherer's emotion component process model [59] can be used to analyze responses to phishing situations. Phished participants appraised the email as a result of a previous mistake (cognitive appraisal), this invoked anxiety and insecurity (subjective feeling); they interrupted their current task (preparation for action), immediately clicked on the phishing-link and provided data (behavioral intention/eventual behavior); the situation was then re-appraised as a solved problem, which invoked pride and satisfaction. The procedural nature of the appraisal theory makes it an excellent tool to assess how emotional processes affect responses to security-critical situations.

We explored emotions as a central predictor for behavior.

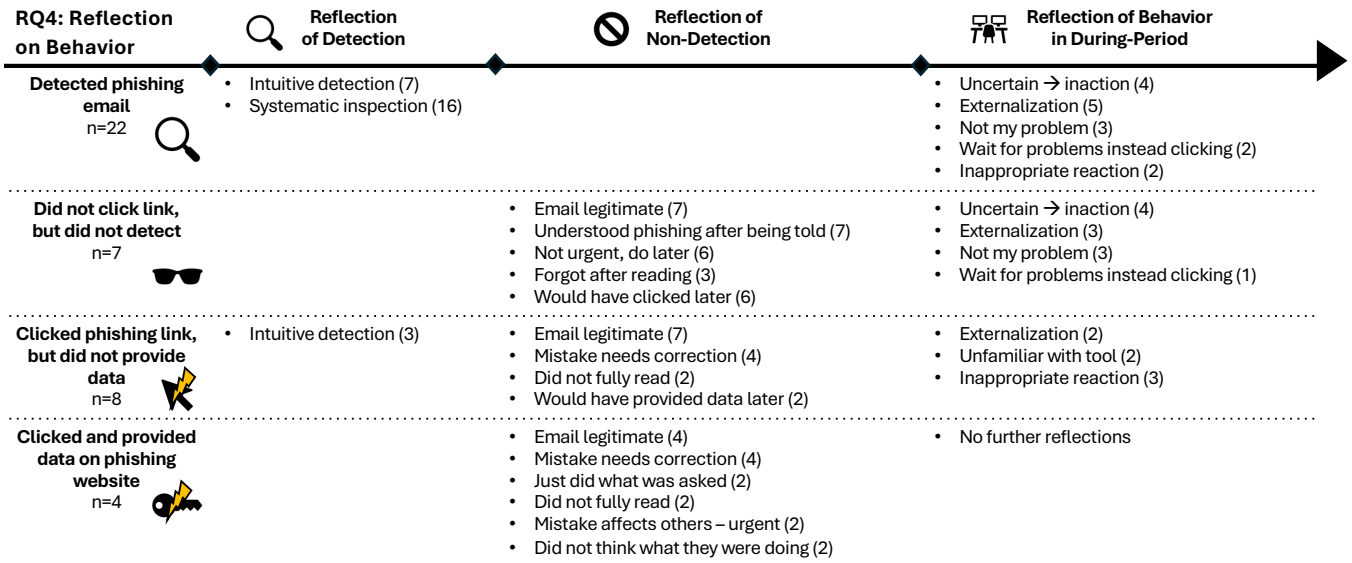


Figure 6: A simplified overview of all reflections on participants' behavior during the phishing attack in chronological order, addressing RQ4. Code frequencies in brackets. Columns refer to respective subsections, rows to participant groups. Bullet-points represent codes.

This is in line with de Kok et al. [17], who found that affective (i.e., emotional) components of attitudes predict behavior better than cognitive ones. In Kahneman's [35] dual system theory, emotions are especially relevant for quick decisions (system 1), which are often apparent in social engineering situations. Understanding security-relevant behavior through the lens of emotional processes can provide nuanced insights and open up new avenues for interventions, a currently underexplored research avenue in human-centered security.

We identified how patterns of emotions influenced reactions to phishing, ultimately highlighting the crucial role of emotions in security behavior: Negative emotions and reappraisal often led to interacting with the phish, especially when participants appraised the phish as resulting from a prior mistake. Participants who did not fall for the phish often followed the process of noticing the interruption, appraising the situation as a phishing attack, and feeling a conflict between suspicion and the possible need to click to complete a task. This led to worry, followed by feeling that they were able to deal with the phish successfully, and satisfaction. While previous studies explored general behavioral tendencies or induced emotions [2, 54, 69], our findings provide initial insights into how emotions play a crucial role in specific security behaviors and decisions, with these emotions emerging from the interaction.

5.2 Methodological Insights for USP Research

Task Scenarios to Study Social Engineering. Our study is, to our best knowledge, the first to simulate a phishing scenario in this level of detail: we created a realistic setting that immersed participants despite disclosing the study topic and content warnings. Comparable studies injected simulated phishing emails in real-life setups, including long-term cover scenarios [46] or workplace observation [22]. As real-life in-situ setups are not always a feasible (or possible) option, our novel method is possibly the closest to reality it can get. This offers compelling opportunities for researchers who wish to study phishing in a risk-free way by keeping deception to a minimum. Our method could benefit qualitative studies on social engineering, which is especially relevant since the small body of research around emotions and phishing is often quantitative (e.g., [2, 13]). The scenario can also be customized (e.g., more interaction, change context, etc.).

Studying Detectors to Enable Secure Behavior. Zimmermann et al. [79] suggested an *enabling approach* to understand how and why people are behaving securely during cyberattacks. Research from other fields also demonstrated that studying successful behavior in combination with emotions could foster positive outcomes. Shiota et al. [65] discovered that interventions simulating the pleasures of physical exercise invoked positive emotions, which was more effective to induce healthy behavior change than fear appeals. This is comparable to our detectors, who experienced satisfaction, pride, and self-efficacy. Emotion-aware, enabling training, could help users strengthen self-efficacy and detection skills.

5.3 Practical Implications for Emotion-Aware Interventions

As emotions and appraisals can impact behavior during phishing, they should be considered in intervention design. We

suggest three ideas for emotion-aware interventions contributing to organizational resilience against social engineering.

From Simulated Phishing Campaigns to Transparent Periodic Training. Simulated phishing provides educational content upon clicking on a phishing link [40]. In line with prior work [67], our participants experienced shame, disappointment, and helplessness after clicking. Learning science argues that shame generally blocks learning [71]. In education settings, negative emotions hinder assistance seeking and lower students' motivation and engagement [56]. Organizations depend on employees' long-term collaboration regarding cybersecurity. Causing negative emotions through phishing simulations can be counterproductive to learning [63].

As an alternative, we suggest openly-communicated periodic trainings, which gently encourage users to practice and fail [71]. Instead of exposing users to a simulated threat, they are periodically presented with examples of current phishing emails, which allow to detect "red flags" in a playful manner.

Our participants reported frustration, annoyance, or uncertainty, because they appraised that not clicking on the phishing link could lead to negative consequences. Planned detection training could eliminate these feelings and instead invoke positive emotions such as pride and confidence, which we found were connected to creating self-efficacy for detection skills. The reoccurring interaction with phishing content additionally benefits users by reminding them of the problem [43].

Scenario-Based Trainings. A scenario setting similar to our methodology could be used to conduct cybersecurity trainings for staff by adapting the context and phishing pretext to the respective organization. After a session, trainees could reflect the session and learn about secure behavior; emotions should be addressed in the reflection to support learning [71]. This offers flexibility for different employees and can benefit those who tend to overestimate their cybersecurity skills [72]. Trainings can also be conducted in teams: one group acts as attackers, being in charge of the phishing emails, while the others work on the tasks. Both groups can learn from each other in the reflection. Role-playing scenarios can increase self-efficacy and intention to seek support in phishing situations [15]. As a further benefit, the majority of our participants noted that the session was fun. Positive emotions experienced during training aid in learning [73] and can reinforce future positive behaviors.

Organizational Culture. Many participants, even detectors, experienced cognitive dissonance when interacting with the phishing email: some appraised it as suspicious, but reappraised that not clicking could impact colleagues negatively (e.g., through delays) – and possibly their own reputation. In an organization, these users would profit from clearly defined phishing policies and a positive culture of handling mistakes, as illustrated by Dupuis et al. [26]. Most importantly, it needs to be made clear that being cautious will not be sanctioned.

As detectors, on the other hand, were often annoyed by phishing emails, they should be encouraged to seek social support (e.g. venting) in order to cope with their emotions and simultaneously share their insights and/or warn others [45].

5.4 Avenues for Future Research

Emotions in Cybersecurity. Our findings demonstrate that considering emotions is a central avenue for understanding why some clicked, provided data, and why others did not. Work in human-centered security often considers cognition and behavior, but emotions remain underresearched [70], despite having impact on both. We hope to see more future work on emotions and emotion-aware interventions in this field.

Considering Negative Emotions in Technical Interventions. For many participants, annoyance led to detection. Breaking the flow and getting a user to switch their attention to a security risk is a well-known, yet unsolved challenge [10]. Forced attention warnings [49, 50] might create annoyance and break the flow, but habituation remains a challenge [25]. Future work could test combinations of technical solutions (see [7]), where the first invokes a slight annoyance and stops the user, while the second aims to compensate for habituation.

Studying Non-Detectors. We identified a group whose importance has not received considerable attention so far: Participants who did not click the link but also did not understand that the email was phishing (non-detectors). As they technically did nothing wrong, they possibly went unnoticed in prior work. All non-detectors have read the email and almost all stated they would have clicked the link later, a behavior observed before [77]. This group is difficult to identify, but warrants further investigation, for example through specific questionnaire items or interview questions after phishing detection tasks.

6 Conclusion

Phishing remains a challenge as attackers' techniques evolve [47,62]. Technical measures alone are insufficient and psychological processes at the moment of a phishing attack are unexplored. We studied these psychological phenomena (emotions, appraisals, and behaviors related to a phishing attack) in a realistic scenario through the lens of emotions with the appraisal theory [59]. Our results show how emotions affect behavior during phishing. Negative emotions and (re-)appraisal led to security-comprising outcomes. Positive emotions were often associated with successful detection and self-efficacy. Our work provides avenues for future research into emotion-aware interventions to increase people's resilience against social engineering.

Acknowledgments

We thank our event coordinator who helped to design scenario and tasks. We thank our shepherd. Interview transcripts were created using the Speech2Text tool from the Aalto University Science-IT project; apart from this, we did not use LLMs/AI.

Availability

The Supplementary Material includes anonymized interview transcripts, quantitative data, and additional detailed descriptions, figures, and tables. It can be accessed via: https://doi.org/10.17605/OSF.IO/HBZCK.

References

[1] Yomna Abdelrahman, Florian Alt, Tilman Dingler, Christopher Hadnagy, Abbie Maroño, and Verena Distler. Defining and Fortifying Against Cognitive Vulnerabilities in Social Engineering (Dagstuhl Seminar 23462). Technical report, Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2024. https://drops.dagstuhl.de/entities/document/10.4230/DagRep.13.11.103.

[2] Hossein Abroshan, Jan Devos, Geert Poels, and Eric Laermans. COVID-19 and Phishing: Effects of Human Emotions, Behavior, and Demographics on the Success of Phishing Attempts During the Pandemic. *IEEE Access*, 9:121916–121929, 2021. https://ieeexplore.ieee.org/document/9525387/.

[3] Hossein Abroshan, Jan Devos, Geert Poels, and Eric Laermans. Phishing happens beyond technology: The effects of human behaviors and demographics on each step of a phishing process. *IEEE Access*, 9:44928–44949, 2021. https://ieeexplore.ieee.org/document/9380285.

[4] Julio Angulo and Martin Ortlieb. "WTH..!?!" experiences, reactions, and expectations related to online privacy panic situations. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, SOUPS '15, page 19–38, USA, 2015. USENIX Association. https://www.usenix.org/conference/soups2015/proceedings/presentation/angulo.

[5] American Psychological Association. Ethical principles of psychologists and code of conduct, 2017. https://www.apa.org/ethics/code.

[6] Eliot Baker and Maxime Cartier. Phishing Trends Report (Updated for 2025), 2025. https://hoxhunt.com/guide/phishing-trends-report.

[7] Benjamin Maximilian Berens, Florian Schaub, Mattia Mossano, and Melanie Volkamer. Better together: The interplay between a phishing awareness video and a link-centric phishing support tool. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery. https://doi.org/10.1145/3613904.3642843.

[8] Marc A. Brackett, Susan E. Rivers, Sara Shiffman, Nicole Lerner, and Peter Salovey. Relating emotional abilities to social functioning: A comparison of self-report and performance measures of emotional intelligence. *Journal of Personality and Social Psychology*, 91(4):780–795, 2006. https://doi.apa.org/doi/10.1037/0022-3514.91.4.780.

[9] Margaret M Bradley and Peter J Lang. The International Affective Picture System (IAPS) in the Study of Emotion and Attention. In James A Coan and John J B Allen, editors, *Handbook of Emotion Elicitation and Assessment*. Oxford University Press, 2007. https://doi.org/10.1093/oso/9780195169157.003.0003.

[10] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W. Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. Your attention please: designing security-decision uis to make genuine risks harder to ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, New York, NY, USA, 2013. Association for Computing Machinery. https://doi.org/10.1145/2501604.2501610.

[11] Adriana Breaban and Charles N Noussair. Emotional State and Market Behavior. *Review of Finance*, 22(1):279–309, 2018. https://academic.oup.com/rof/article/22/1/279/3870423.

[12] Lina Brunken, Annalina Buckmann, Jonas Hielscher, and M. Angela Sasse. "To do this properly, you need more resources": the hidden costs of introducing simulated phishing campaigns. In *Proceedings of the 32nd USENIX Conference on Security Symposium*, SEC '23, USA, 2023. USENIX Association. https://www.usenix.org/conference/usenixsecurity23/presentation/brunken.

[13] Sanja Budimir, Johnny R.J. Fontaine, and Etienne B. Roesch. Emotional Experiences of Cybersecurity Breach Victims. *Cyberpsychology, Behavior, and Social Networking*, 24(9):612–616, September 2021. https://www.liebertpub.com/doi/10.1089/cyber.2020.0525.

[14] Pavlo Burda, Luca Allodi, and Nicola Zannone. Cognition in social engineering empirical research: A systematic literature review. *ACM Trans. Comput.-Hum. Interact.*, 31(2), January 2024. https://doi.org/10.1145/3635149.

[15] Xiaowei Chen, Margault Sacré, Gabriele Lenzini, Samuel Greiff, Verena Distler, and Anastasia Sergeeva. 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 2024 CHI Conference on Human Factors in Computing Systems*, CHI '24, New York, NY, USA, 2024. Association for Computing Machinery. https://doi.org/10.1145/3613904.3641943.

[16] Claes Dahlqvist. Cognitive and motivational qualities of task instruction: Cognitive appraisals and achievement emotions of Swedish primary teacher students. *The Journal of Academic Librarianship*, 49(6):102797, November 2023. https://linkinghub.elsevier.com/retrieve/pii/S0099133323001362.

[17] Lisa C. de Kok, Deborah Oosting, and Marc A. H. Spruit. The influence of knowledge and attitude on intention to adopt cybersecure behaviour. *Information & Security: An International Journal*, 2020. https://isij.eu/system/files/download-count/2023-01/4618_cybrsecure_behaviour.pdf.

[18] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06, page 581–590, New York, NY, USA, 2006. Association for Computing Machinery. https://doi.org/10.1145/1124772.1124861.

[19] APA Dictionary. Emotion, April 2018. https://dictionary.apa.org/emotion.

[20] APA Dictionary. Feeling, April 2018. https://dictionary.apa.org/feeling.

[21] APA Dictionary. Mood, April 2018. https://dictionary.apa.org/mood.

[22] Verena Distler. 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*, CHI '23, New York, NY, USA, 2023. Association for Computing Machinery. https://doi.org/10.1145/3544548.3581170.

[23] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig. A systematic literature review of empirical methods and risk representation in usable privacy and security research. *ACM Trans. Comput.-Hum. Interact.*, 28(6), 2021. https://doi.org/10.1145/3469845.

[24] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Vincent Koenig, and Lorrie Faith Cranor. Empirical Research Methods in Usable Privacy and Security. In Nina Gerber, Alina Stöver, and Karola Marky, editors, *Human Factors in Privacy Research*, pages 29–53. Springer International Publishing, Cham, 2023. https://doi.org/10.1007/978-3-031-28643-8_3.

[25] Verena Distler, Gabriele Lenzini, Carine Lallemand, and Vincent Koenig. The Framework of Security-Enhancing Friction: How UX Can Help Users Behave More Securely. In *Proceedings of the New Security Paradigms Workshop 2020*, NSPW '20, page 45–58, New York, NY, USA, 2021. Association for Computing Machinery. https://doi.org/10.1145/3442167.3442173.

[26] Marc Dupuis, Rosalind Searle, and Karen V. Renaud. Finding grace in responses to adverse cybersecurity incidents. *Journal of Intellectual Capital*, 26(1):45–70, 2025. https://www.emerald.com/insight/content/doi/10.1108/JIC-04-2024-0128/full/html.

[27] Michael Eid. Advanced Statistical Methods for the Study of Appraisal and Emotional Reaction. In Klaus R. Scherer, Angela Schorr, and Tom Johnstone, editors, *Appraisal Processes in Emotion: Theory, Methods, Research*, pages 319–330. Oxford Academic, New York, NY, 2023. https://academic.oup.com/book/53557/chapter/422116061.

[28] Michael Fagan, Yusuf Albayram, Mohammad Maifi Hasan Khan, and Ross Buck. An investigation into users' considerations towards using password managers. *Human-centric Computing and Information Sciences*, 7(1):12, 2017. https://link.springer.com/10.1186/s13673-017-0093-6.

[29] Waldo Rocha Flores, Hannes Holm, Marcus Nohlberg, and Mathias Ekstedt. An Empirical Investigation of the Effect of Target-Related Information in Phishing Attacks. In *2014 IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations*, pages 357–363. IEEE, 2014. https://ieeexplore.ieee.org/document/6975383/.

[30] William J Gordon, Adam Wright, Robert J Glynn, Jigar Kadakia, Christina Mazzone, Elizabeth Leinbach, and Adam Landman. Evaluation of a mandatory phishing training program for high-risk employees at a us healthcare system. *Journal of the American Medical Informatics Association*, 26(6):547–552, 2019. https://pubmed.ncbi.nlm.nih.gov/30861069/.

[31] Francesco Greco, Giuseppe Desolda, Paolo Buono, and Antonio Piccinno. Enhancing Phishing Defenses: The Impact of Timing and Explanations in Warnings for Email Clients. *Computer Standards & Interfaces*, 93:103982, 2025. https://linkinghub.elsevier.com/retrieve/pii/S092054892500011X.

[32] Katharine H. Greenaway, Elise K. Kalokerinos, and Lisa A. Williams. Context is Everything (in Emotion Research). *Social and Personality Psychology Compass*, 12(6):e12393, 2018.

https://compass.onlinelibrary.wiley.com/doi/10.1111/spc3.12393.

[33] Deanna House and M. K. Raja. Phishing: message appraisal and the exploration of fear and self-confidence. *Behaviour & Information Technology*, 39(11):1204–1224, 2020. https://www.tandfonline.com/doi/full/10.1080/0144929X.2019.1657180.

[34] IBM. Cost of a data breach report 2025, 2025. https://www.ibm.com/reports/data-breach.

[35] Daniel Kahneman. *Thinking, Fast and Slow*. Farrar, Straus and Giroux, New York, first paperback edition, 2011. https://psycnet.apa.org/record/2011-26535-000.

[36] S. Kavya and D. Sumathi. Staying ahead of phishers: a review of recent advances and emerging methodologies in phishing detection. *Artificial Intelligence Review*, 58(2):50, 2024. https://link.springer.com/10.1007/s10462-024-11055-z.

[37] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A. Martucci. Enhancing privacy through the visual design of privacy notices: exploring the interplay of curiosity, control and affect. In *Proceedings of the Sixteenth USENIX Conference on Usable Privacy and Security*, SOUPS'20, USA, 2020. USENIX Association. https://www.usenix.org/conference/soups2020/presentation/kitkowska.

[38] Udo Kuckartz and Anne McWhertor. *Qualitative text analysis: a guide to methods, practice & using software*. SAGE, Los Angeles, 2014. https://www.researchgate.net/publication/365070976_Qualitative_Text_Analysis_A_Guide_to_Methods_Practice_Using_Software.

[39] Udo Kuckartz and Stefan Rädiker. *Analyzing Qualitative Data with MAXQDA: Text, Audio, and Video*. Springer International Publishing, Cham, 2019. https://link.springer.com/10.1007/978-3-030-15671-8.

[40] Ponnurangam Kumaraguru, Lorrie Cranor, and Laura Mather. Anti-phishing landing page: Turning a 404 into a teachable moment for end users. In *Sixth Conference on Email and Anti-Spam*, 07 2009. https://www.researchgate.net/publication/228846483_Anti-Phishing_Landing_Page_Turning_a_404_into_a_Teachable_Moment_for_End_Users.

[41] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, New York, NY, USA, 2009. Association for Computing Machinery. https://doi.org/10.1145/1572532.1572536.

[42] Ponnurangam Kumaraguru, Yong Rhee, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Protecting people from phishing: the design and evaluation of an embedded training email system. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '07, page 905–914, New York, NY, USA, 2007. Association for Computing Machinery. https://doi.org/10.1145/1240624.1240760.

[43] Daniele Lain, Tarek Jost, Sinisa Matetic, Kari Kostiainen, and Srdjan Capkun. Content, nudges and incentives: A study on the effectiveness and perception of embedded phishing training. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, CCS '24, page 4182–4196, New York, NY, USA, 2024. Association for Computing Machinery. https://doi.org/10.1145/3658644.3690348.

[44] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 842–859, San Francisco, CA, USA, 2022. IEEE. https://ieeexplore.ieee.org/document/9833766/.

[45] Huigang Liang, Yajiong Xue, Alain Pinsonneault, and Yu "Andy" Wu. What Users Do Besides Problem-Focused Coping When Facing It Security Threats: An Emotion-focused Coping Perspective. *MIS Quarterly*, 43(2):373–393, June 2019. https://doi.org/10.25300/MISQ/2019/14360.

[46] Rhian Lukins, Neeranjan Chitare, Nalin Arachchilage, Lynne Coventry, and James Nicholson. When Trust Overrides Caution: Investigating Spear Phishing in Personal Contexts Among Young and Older Adults. In *2025 European Symposium on Usable Security (EuroUSEC)*, pages 76–85, Manchester, United Kingdom, September 2025. IEEE. https://ieeexplore.ieee.org/document/11300480/.

[47] Nikol Mashtalyar, Uwera Nina Ntaganzwa, Thales Santos, Saqib Hakak, and Suprio Ray. Social Engineering Attacks: Recent Advances and Challenges. In Abbas Moallem, editor, *HCI for Cybersecurity, Privacy and Trust*, volume 12788, pages 417–431. Springer International Publishing, Cham, 2021. https://link.springer.com/10.1007/978-3-030-77392-2_27.

[48] Kevin D Mitnick and William L Simon. *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2003. https://www.researchgate.net/publication/234806566_The_Art_of_Deception_Controlling_the_Human_Element_of_Security.

[49] Justin Petelka, Benjamin Berens, Carlo Sugatan, Melanie Volkamer, and Florian Schaub. Restricting the Link: Effects of Focused Attention and Time Delay on Phishing Warning Effectiveness. In *2025 IEEE Symposium on Security and Privacy (SP)*, pages 1–19, San Francisco, CA, USA, 2025. IEEE. https://ieeexplore.ieee.org/document/11023395/.

[50] Justin Petelka, Yixin Zou, and Florian Schaub. Put your warning where your link is: Improving and evaluating email phishing warnings. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–15, New York, NY, USA, 2019. Association for Computing Machinery. https://doi.org/10.1145/3290605.3300748.

[51] Karen S. Quigley, Kristen A. Lindquist, and Lisa Feldman Barrett. Inducing and Measuring Emotion and Affect: Tips, Tricks, and Secrets. In Harry T. Reis and Charles M. Judd, editors, *Handbook of Research Methods in Social and Personality Psychology*, pages 220–252. Cambridge University Press, 2 edition, 2014. https://www.cambridge.org/core/product/identifier/9780511996481%23c01177-2742/type/book_part.

[52] Karen S Quigley, Kristen A Lindquist, and Lisa Feldman Barrett. Inducing and measuring emotion and affect: Tips, tricks, and secrets. *Handbook of research methods in social and personality psychology*, 2:220–252, 2014. https://psycnet.apa.org/record/2014-12227-010.

[53] Karen Renaud, Rosalind Searle, and Marc Dupuis. Cybersecurity regrets: I've had a few.... je ne regrette. In *Proceedings of the 2022 New Security Paradigms Workshop*, NSPW '22, page 1–20, New York, NY, USA, 2023. Association for Computing Machinery. https://doi.org/10.1145/3584318.3584319.

[54] Karen Renaud, Verena Zimmermann, Tim Schürmann, and Carlos Böhm. Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, 8(1):75, 2021. https://www.nature.com/articles/s41599-021-00746-5.

[55] Heather Rosoff, Jinshu Cui, and Richard John. Behavioral experiments exploring victims' response to cyber-based financial fraud and identity theft scenario simulations. In *Proceedings of the Tenth USENIX Conference on Usable Privacy and Security*, SOUPS '14, page 175–186, USA, 2014. USENIX Association. https://www.usenix.org/conference/soups2014/proceedings/presentation/rosoff.

[56] Anna D. Rowe and Julie Fitness. Understanding the Role of Negative Emotions in Adult Learning and Achievement: A Social Functional Perspective. *Behavioral Sciences*, 8(2):27, February 2018. https://www.mdpi.com/2076-328X/8/2/27.

[57] James A. Russell. A circumplex model of affect. *Journal of Personality and Social Psychology*, 39(6):1161–1178, 1980. https://doi.apa.org/doi/10.1037/h0077714.

[58] James A. Russell and Lisa Feldman Barrett. Core affect, prototypical emotional episodes, and other things called emotion: Dissecting the elephant. *Journal of Personality and Social Psychology*, 76(5):805–819, 1999. https://doi.apa.org/doi/10.1037/0022-3514.76.5.805.

[59] Klaus R. Scherer. What are emotions? And how can they be measured? *Social Science Information*, 44(4):695–729, December 2005. https://journals.sagepub.com/doi/10.1177/0539018405058216.

[60] Klaus R. Scherer, Vera Shuman, Johnny R. J. Fontaine, and Cristina Soriano. The GRID meets the Wheel: Assessing emotional feeling via self-report. In Johnny R. J. Fontaine, Klaus R. Scherer, and Cristina Soriano, editors, *Components of Emotional Meaning*, pages 281–298. Oxford University Press, 2013. https://academic.oup.com/book/2214/chapter/142269657.

[61] Katja Schlegel, Vera Shuman, and Klaus Scherer. Geneva Emotion Wheel Rating Study. Unpublished report, 2012. https://www.unige.ch/cisa/application/files/4514/6720/4016/Geneva_Emotion_Wheel_Rating_Study_Report_2012_08_11_2.0.pdf.

[62] Marc Schmitt and Ivan Flechais. Digital deception: generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, 57(12):324, 2024. https://link.springer.com/10.1007/s10462-024-10973-2.

[63] Jasmin Schwab, Alexander Nussbaum, Anastasia Sergeeva, Florian Alt, and Verena Distler. What Makes Phishing Simulation Campaigns (Un)Acceptable? A Vignette Experiment. In *Proceedings 2025 Symposium on Usable Security*, San Diego, CA, USA, 2025. Internet Society. https://www.ndss-symposium.org/wp-content/uploads/usec25-10.pdf.

[64] Michelle N Shiota, Esther K Papies, Stephanie D Preston, and Disa A Sauter. Positive affect and behavior change. *Current Opinion in Behavioral Sciences*, 39:222–228, 2021. https://linkinghub.elsevier.com/retrieve/pii/S235215462100108X.

[65] Michelle N. Shiota, Carley Vornlocher, and Lile Jia. Emotional Mechanisms of Behavior Change: Existing Techniques, Best Practices, and a New Approach. *Policy Insights from the Behavioral and Brain Sciences*, 10(2):201–211, October 2023. http://journals.sagepub.com/doi/10.1177/23727322231195907.

[66] Craig Smith and Phoebe Ellsworth. Patterns of cognitive appraisal in emotion. *Journal of personality and social psychology*, 48:813–38, 05 1985. https://www.researchgate.net/publication/19274815_Patterns_of_Cognitive_Appraisal_in_Emotion.

[67] Jan Tolsdorf, David Langer, and Luigi Lo Iacono. Phishing susceptibility and the (in-)effectiveness of common anti-phishing interventions in a large university hospital. In *Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security*, CCS '25, page 4334–4348, New York, NY, USA, 2025. Association for Computing Machinery. https://doi.org/10.1145/3719027.3765164.

[68] Melanie Volkamer, Martina Angela Sasse, and Franziska Boehm. Analysing simulated phishing campaigns for staff. In *Computer Security: ESORICS 2020 International Workshops, DETIPS, DeSECSys, MPS, and SPOSE, Guildford, UK, September 17–18, 2020, Revised Selected Papers*, page 312–328, Berlin, Heidelberg, 2020. Springer-Verlag. https://doi.org/10.1007/978-3-030-66504-3_19.

[69] Alexandra von Preuschen, Monika C. Schuhmacher, and Verena Zimmermann. Beyond fear and frustration - towards a holistic understanding of emotions in cybersecurity. In *Twentieth Symposium on Usable Privacy and Security, SOUPS 2024*, pages 623–642, Philadelphia, PA, 2024. USENIX Association. https://www.usenix.org/conference/soups2024/presentation/von-preuschen.

[70] Alexandra von Preuschen, Verena Zimmermann, and Monika C. Schuhmacher. How do you Feel about Cybersecurity? – A Literature Review on Emotions in Cybersecurity. In Nina Gerber and Verena Zimmermann, editors, *International Symposium on Technikpsychologie (TecPsy) 2023*, pages 1–13. Sciendo, 2023. https://www.sciendo.com/chapter/9788366675896/10.2478/9788366675896-001.

[71] Jude Walker. Shame and Transformation in the Theory and Practice of Adult Learning and Education. *Journal of Transformative Education*, 15(4):357–374, October 2017. https://journals.sagepub.com/doi/10.1177/1541344617699591.

[72] Jingguo Wang, Yuan Li, and H. Raghav Rao. Overconfidence in Phishing Email Detection. *Journal of the Association for Information Systems*, 17(11):759–783, November 2016. http://aisel.aisnet.org/jais/vol17/iss11/1/.

[73] Xiaoling Wang, Wan Marzuki Wan Jaafar, and Rose Manisah Sulong. Building better learners: exploring positive emotions and life satisfaction as keys to academic engagement. *Frontiers in Education*, 10:1535996, March 2025. https://www.frontiersin.org/articles/10.3389/feduc.2025.1535996/full.

[74] Rick Wash. How experts detect phishing scam emails. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2), October 2020. https://doi.org/10.1145/3415231.

[75] Katherine Williamson and Erik Thulin. Leveraging emotion-behavior pathways to support environmental behavior change. *Ecology and Society*, 27, 2022. https://ecologyandsociety.org/vol27/iss3/art27/.

[76] Carly Wilson and David Argles. The fight against phishing: Technology, the end user and legislation. In *International Conference on Information Society (i-Society 2011)*, pages 501–504, 2011. https://ieeexplore.ieee.org/document/5978553.

[77] Sijie Zhuo, Robert Biddle, Lucas Betts, Nalin Asanka Gamagedara Arachchilage, Yun Sing Koh, Giovanni Russello, Danielle Lottridge, and Robert Biddle. The Impact of Workload on Phishing Susceptibility: An Experiment. In *Proceedings 2024 Symposium on Usable Security*, San Diego, CA, USA, 2024. Internet Society. https://www.ndss-symposium.org/ndss-paper/auto-draft-503/.

[78] Sijie Zhuo, Robert Biddle, Yun Sing Koh, Danielle Lottridge, and Giovanni Russello. Sok: Human-centered phishing susceptibility. *ACM Transactions on Privacy and Security*, 26(3), April 2023. https://doi.org/10.1145/3575797.

[79] Verena Zimmermann, Lorin Schöni, Thierry Schaltegger, Benjamin Ambuehl, Melanie Knieps, and Nico Ebert. Human-centered cybersecurity revisited: From enemies to partners. *Communications of the ACM*, 67:72–81, 2024. https://dl.acm.org/doi/10.1145/3665665.

Appendices

Table 3: Definitions of key terms related to emotions.

Term	Definition
Emotion	Complex reaction pattern involving experiential, behavioral, and physiological elements, to deal with an event [19], or sensory input; appraisal driven; short-lived [59].
Affect	Reaction to a stimulus, either positive or negative (valence), in a certain strength (arousal) [57]; not necessarily invoking a communicable emotion or feeling [51]; not inevitably directed at anything [58].
Feeling	A person's self-contained, subjective experience of an emotion [59]; purely mental component of an emotion [20].
Mood	Emotional state of low intensity, which can be sustained for several days [21]; may arise without apparent reason [59].
Preference	A stable and evaluative positive or negative judgment about a stimulus; generated by intrinsic appraisal and usually independent of current needs or goals; results in unspecific feelings with low behavioral impact [59].

Table 4: An illustration of emotion components in the emotion-appraisal process [59].

Emotion component	Process example
Appraisal	An email impersonates my supervisor and asks for secret information – it could be phishing – I should show my supervisor.
Bodily symptoms	Heart rate increases.
Preparation for action	Interrupt current behavior; re-read email to make sure.
Behavioral intention	Go to supervisor and show them the email.
Subjective feelings	Insecurity, stress.

Table 5: Brief description of participant tasks for the laboratory session. Names, places, and email-addresses have been anonymized.

No.	Task
1	Write arrival instructions to [*event location*] for guests. Include arrival via Metro and parking spaces. Send result to event coordinators team.
2	Create two Zoom-meeting links and send them to event speakers. Write a short email text that can be sent with the link.
3	Create a sign-up questionnaire for the event using Webropol. Send result link to your supervisor.
4	Organize a birthday gift for a colleague. Other colleagues will send you gift ideas via email during the next hour. Collect some good ideas and send them to your colleague.
5	We would like to invite all speakers for dinner. Email travel-events@*university.com* and ask them to get an offer for a three-course dinner from a restaurant of your choice for 20 people.
6	Look up the route to [*after party location*]. How to get there via public transport on a Saturday night? Are there any busy streets to cross? Are there route alternatives? Send result to event coordinators team.
7	Book a room for a meeting for the following day by phone call.
8	Design an invitation email template for guest invitations. Send result to your supervisor.
9	Find the prices for a list of items on external websites. Send the best deals to event coordinators team.
10	Find maps and accessibility info for [*after party location building*] on university website. Send results to your supervisor.

Table 6: The ten most frequently selected emotions before the session (all participants), and during-phishing (split by participant groups). Participants could choose multiple emotions on the questionnaire.

BEFORE (N=41)	**Freq.**	**Detectors (n=22)**	**Freq.**	**Non-detectors (n=7)**	**Freq.**	**Clickers (n=8)**	**Freq.**	**Phished (n=4)**	**Freq.**
Curious	34	Annoyed	16	In the flow	5	Surprised	6	In the flow	3
Calm	33	Curious	12	Active	4	Active	5	Active	2
Interested	33	Surprised	11	Curious	4	Worried	5	Involved	2
Relaxed	28	Confused	10	Satisfied	3	Confused	5	Unconcerned	2
Optimistic	28	Nervous	9	Grateful	3	Curious	4	Anxious	2
Enthusiastic	25	Insecure	9	Calm	3	Tense	4	Satisfied	1
Secure	22	In the flow	8	Happy	3	Anxious	4	Enthusiastic	1
Involved	22	Tense	8	Trust	3	Disappointed	4	Passionate	1
Trust	22	Worried	8	Worried	3	Nervous	4	Relaxed	1
Active	21	Indifferent	7	Enthusiastic	2	Interested	3	Fascinated	1

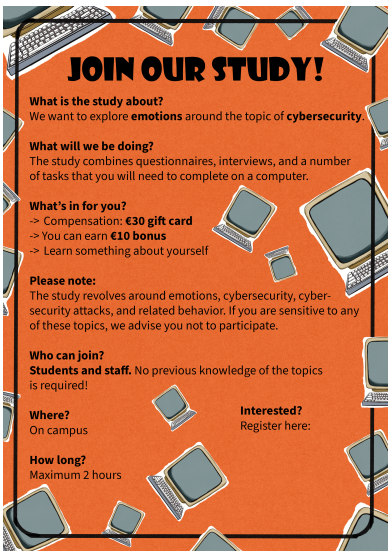


Figure 7: Recruitment poster for our study (names, places, and QR-code have been removed).

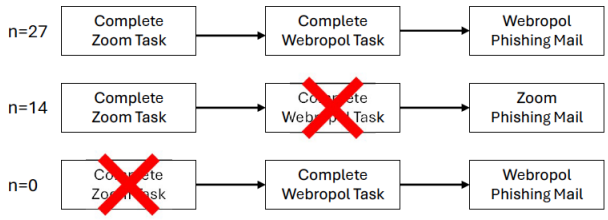
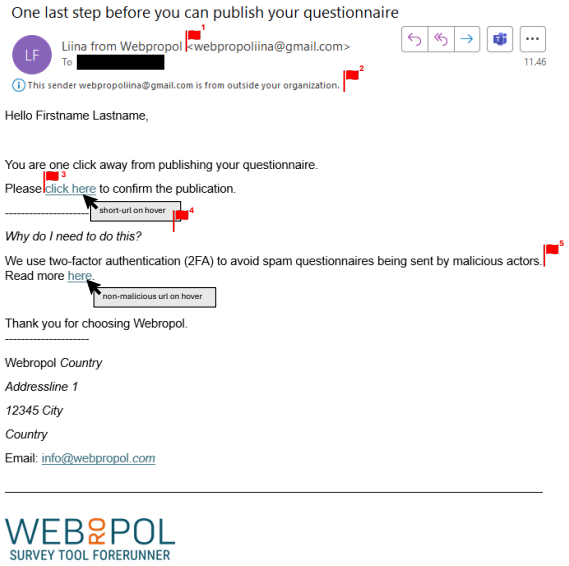


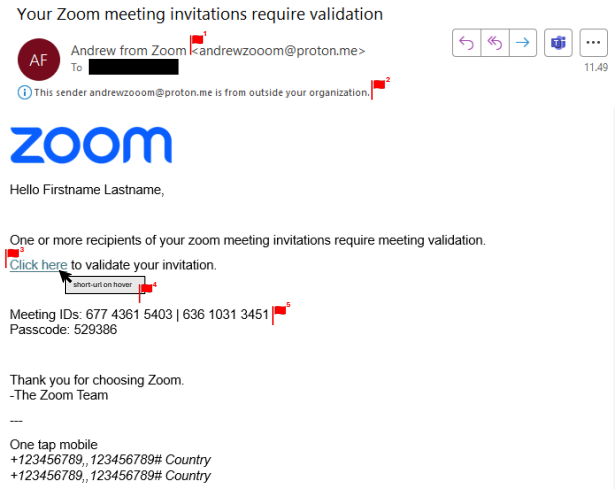
Figure 8: Decision process on what participant received which phishing email. By default, participants received the Webropol email. If they were not able to finish the Webropol task, they received the Zoom phish (and vice-versa).



Figure 9: Study setup resembling a typical office in Aalto University. As new employees, participants received a clean and empty desk and were allowed to utilize it as they wished (work with documents or take notes on paper, etc.). Participants worked alone, but distractions were introduced during the session to create a more realistic environment (see Section 3.4.5). A webcam on a tripod was utilized to observe participants during the session.



(a) Simulated phishing email from Webropol.



(b) Simulated phishing email from Zoom.

Figure 10: The two phishing emails used in the laboratory session. Every participant received one of them, as explained in Section 3.4.6. For illustrative purposes, we added red flag symbols to indicate how participants could have detected the email as phishing (participants did not see the symbols). Red flags as follows (for both emails): 1. generic mail-address domain, 2. "external email"-warning, 3. demand to click on a hidden url, 4. short-url on hover, 5. body text vague, IDs nonsensical. Addresses, phone numbers and names have been anonymized.

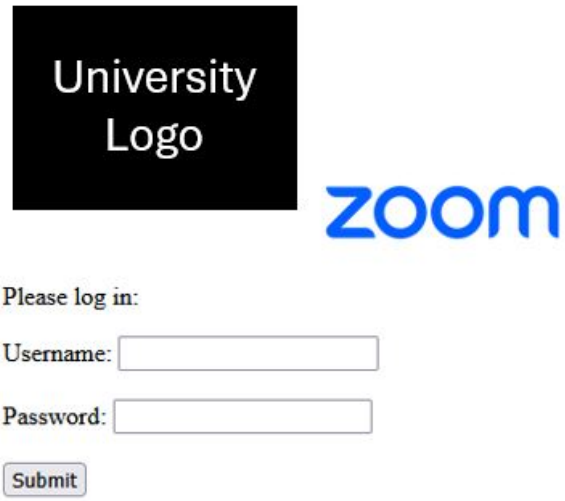


Figure 11: The Zoom-version of the mock website that appeared when a participant clicked on the link in the phishing email. Note: The Webropol-version displayed the Webropol logo.

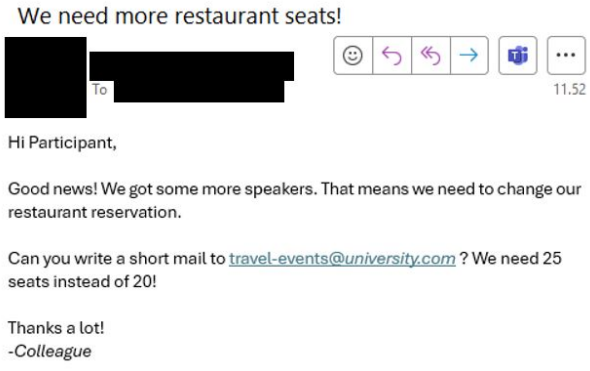


Figure 12: An example of a task-related email participants received during the session. These were introduced as distractions (cf. Section 3.4.5).