

# Department-Specific Security Awareness Campaigns: A Cross-Organizational Study of HR and Accounting

Matthias Pfister\*, Giovanni Apruzzese\*<sup>†</sup>, Irdin Pekaric\*

\*University of Liechtenstein, Vaduz, Liechtenstein; <sup>†</sup>Reykjavik University, Reykjavik, Iceland  
{matthias.pfister, giovanni.apruzzese, irdin.pekaric}@uni.li

**Abstract**—Many cyberattacks succeed because they exploit flaws at the human level. To address this problem, organizations rely on security awareness programs, which aim to make employees more resilient against social engineering. While some works have, implicitly or explicitly, suggested that such programs should account for contextual relevance, the common praxis in research is to adopt a “general” viewpoint. For instance, instead of focusing on department-specific issues, prior user studies sought to provide organization-wide conclusions by treating all participants equally. Such a protocol may lead to overlooking vulnerabilities that affect only specific subsets of an organization, and which can be (or are) exploited by real-world attackers.

In this paper, we tackle such an oversight. First, through a systematic literature review encompassing over 1k papers, we provide factual evidence that prior literature poorly accounted for department-specific needs. Then, building on this (worrying) finding, we carry out a multi-company and mixed-methods study focusing on two pivotal departments of modern organizations: human resources (HR) and accounting. We explore three dimensions: what specific threats are faced by these departments; what topics should be covered in the security-awareness campaigns delivered to these departments; and which delivery methods would maximize the effectiveness of such campaigns for these departments. We begin by interviewing 16 employees of a multinational enterprise, and then use these results as a scaffold to design a structured survey through which we collect the responses of over 90 HR/accounting members of 9 organizations of varying size. We find that HR and accounting departments face distinct threats: HR is targeted through job applications containing malware and executive impersonation, while accounting is exposed to invoice fraud, credential theft, and ransomware. Current training is often viewed as too generic, with employees preferring shorter, scenario-based formats like videos and simulations. These preferences contradict the common industry practice of lengthy, annual sessions. Based on these insights, we propose practical recommendations for designing awareness programs tailored to departmental needs and workflows.

## I. INTRODUCTION

The cybercrime landscape is constantly evolving [1–4], and automated countermeasures cannot ensure protection against the plethora of threats that may target modern organizations [5]. While security mechanisms such as firewalls, intrusion detection systems, as well as encrypted communications, still represent a critical component of a secure infrastructure, real-world evidence has shown that most security violations stem from human (mis)behavior [6]. Indeed, despite decades of efforts focused on countering social-engineering attempts [7–9], the reality is that phishing still works very well [6, 10–14].

For instance, recent research and technical reports (e.g., [6, 15]) show that attackers now craft their phishing hooks by leveraging large-language models (LLM), or by embedding malicious quick-response (QR) codes in emails—both being means that simultaneously (i) evade existing “machine-based” countermeasures, and (ii) deceive human users. These threats are further emphasized by the variety of available tools usable to convey phishing attacks [16, 17].

From a technical viewpoint, it is now acknowledged that development of a perfect detection mechanism against cyberattacks is an unfeasible objective [8]. Given the economics of cybercrime [18–20] (which caused \$15+ billions of losses just in 2024 [5]), attackers are highly incentivized to circumvent any automated defense that may be adopted by organizations [21]. Therefore, abundant attention has been given to *human-centered* countermeasures—such as phishing education, awareness, and training campaigns [22–24]. For instance, a 2024 survey across 15 countries and encompassing 1050 security professionals and 7500 end users, revealed that 99% of the respondents had some sort of security awareness program in their companies [6]. Yet, barely half (53%) of the respondents asserted that such program was administered to everyone in the respective organization. This finding begs the question “could it be that the persisting effectiveness of phishing is due to an uneven treatment of phishing education across a company’s departments?”

Abundant prior work has shown that such educational campaigns do generally yield more resilient employees [25, 26], which translates to an improved cybersecurity culture of the corresponding organization and, hence, potentially leading to an increased protection against social-engineering attacks [15]. For instance, an employee who quickly reports a phishing email (or talks about receiving a suspicious email [27]) can protect their entire company against the corresponding attack [28]. However, if such a phishing email is sent only to a select number of individuals (e.g., those confined to a specific department of an organization) who did not receive adequate training, then such an oversight may put the entire organization at risk of a data breach [29]. In other words, what matters is not “delivering phishing trainings” (which is allegedly done by almost all organizations [6]), but rather, “ensuring that such trainings are delivered, and tailored, to all departments—especially those more prone to being targeted

by phishing attacks”. Our work is rooted on this principle.

Some research does support such an assertion. For instance, the well-known S&P’22 and CCS’24 papers by Lain et al. highlight that long-term phishing resilience requires alignment with employees’ actual roles and exposure [22], and that phishing training is most effective when the content is aligned with users’ motivations and job functions [23]. From a different angle, Burda et al. [30] and Meurs et al. [31], show that attackers exploit department-specific communication patterns to craft their phishing emails—indicating that awareness campaigns should be designed to counter such department-specific phishing threats. Even the 2020 extensive literature review in [25] concluded that phishing-training exercises should be adjusted according to the specific employees. And yet, as we will show, the common practice in research is to focus on “general” assessments—a habit which does not allow to elucidate department-specific needs and vulnerabilities related to social-engineering threats. This paper seeks to provide evidence of, and then rectify, such a research gap.

**RESEARCH DESIGN AND MAJOR FINDINGS.** There is limited evidence suggesting that prior literature accounted for department-specific issues in cybersecurity awareness campaigns. Our aim is to propose a set of guidelines and recommendations on how to build targeted cybersecurity campaigns focusing on HR and accounting departments. Let us summarize our work, which encompasses three research activities:

- As a first step, we conduct a systematic literature review by applying keyword-based search and snowballing methodologies. We analyze 1219 papers and identify 29 relevant papers. We find that previous works recognize the importance of tailoring awareness campaigns to the needs of specific audiences. Despite this recognition, organizations still continue to rely on generic awareness campaigns that do *not consider differences* in job roles, existing knowledge levels or cultural contexts. Moreover, existing studies *overlook the importance of real-world organizational context*.
- We then carry out interviews with 16 employees from HR, accounting, and cybersecurity departments, exploring specific threat perceptions, knowledge gaps, training needs, and delivery preferences. We qualitatively analyze the responses and find that exploitation techniques differ substantially across departmental processes and data types. We also highlight a subtle threat: *malware embedded in fake job applications* delivered via hiring platforms and email attachments—a tactic specifically tailored to HR workflows. Notably, we did not identify any prior literature that explicitly documents or investigates this specific attack vector.
- By using our interviews as a scaffold, we design and distribute a structured survey to 93 employees of 9 organizations. Our quantitative analyses reveal statistically significant differences in threat awareness, training format preferences and behavioral barriers between departments. Importantly, we find that participants favored *quarterly training sessions* with video and scenario-driven content.

Additional findings demonstrated low awareness of emerging

cyber threats. This suggests that training materials are not updated frequently, which is a gap confirmed by participants who acknowledged repetitive content in past sessions. This misalignment with best practices that recommend regular updates could explain the low impact of generic campaigns.

Based on our findings, we recommend shifting from a “one-size-fits-all” to a “fit-for-context” model of cybersecurity awareness. Our findings are particularly relevant for practitioners in security operations, risk management, and law enforcement, as well as policymakers aiming to foster secure digital behavior in critical sectors. Thus, this work bridges the gap between academic research and practice by offering evidence-based recommendations to enhance the efficacy of cybersecurity awareness campaigns.

**CONTRIBUTIONS.** We contribute to cybercrime research by:

- showing that prior work on cybersecurity awareness overlooked department-specific issues of modern organizations;
  - carrying out a mixed-methods and multi-organizational user study focusing on various aspects of cybersecurity awareness programs in HR and accounting departments;
  - providing recommendations based on our original findings.
- For transparency, we provide low-level details of our research methods (e.g., questionnaire and interview guides) in the Appendix. We also share additional resources in our repository: <https://github.com/irdin-pekaric/eCrime2025>.

## II. RELATED WORK AND MOTIVATION

We summarize cybersecurity awareness programs, and briefly position HR and accounting in the cybercrime landscape (§II-A). Then, we present our systematic literature review (§II-B), and define the research gap (§II-C).

### A. Background

Organizations invest a massive amount of resources in cybersecurity measures to defend against a diverse range of threats [2, 32]. However, it has been shown that currently-deployed “machine-based” countermeasures can be evaded easily (e.g., [15, 33, 34]). Therefore, cybersecurity awareness programs now represent a pivotal asset in the overall security infrastructure of modern organizations [24, 35, 36].

**1) Cybersecurity Awareness Campaigns:** These activities<sup>1</sup> seek to inform and educate employees on various cybersecurity threats, with the purpose of enabling employees to recognize and respond to malicious actions, policy violations and other security-noteworthy events [35]. Traditional awareness programs rely on a variety of approaches, including newsletters, static e-learning modules, or even attack simulations [15, 38, 39]. It has been found that employees undergoing such awareness programs do indeed improve their security attitude [22, 40, 41]. However, various prior work have also

<sup>1</sup>We use the term “awareness”, but other terms exist, such as “training” and “education.” From a semantical standpoint, the “awareness” is necessary to both “training” and “education” (i.e., you cannot “educate” or “train” an employee if they are not “aware” of a given threat [37]) which is why we will use the term “awareness” in the remainder of this paper.

criticized similar approaches, since they can lead to a false-sense of security (e.g., employees may show improvements in “tests”, but may still fail “in practice” [24]), and may lead to a reduced productivity (or increased stress), since employees must tend to such educational activities on top of the tasks pertaining their actual role in an organization [42]. Put simply, despite their potential effectiveness, security awareness programs present much room for improvement.

**2) Threats to HR and Accounting:** These departments have a strategic role in modern organizations due to their access to personal and financial data. As such, they often serve as gateways to sensitive assets, information, and communication flows—making these departments rather attractive targets for attackers. Social engineering techniques – which can trick employees into revealing credentials, downloading malicious attachments or authorizing fraudulent transactions – often target HR workflows that include recruitment or employee onboarding, which exposes staff to external communications [43]. For instance, attackers may leverage fictitious resumes to impersonate applicants [44]. In parallel, the workflows of accounting departments (such as vendor payments and payroll processing) are particularly prone to exploitation due to their urgency and perceived authority. Common well-known techniques include Business Email Compromise (BEC), invoice fraud and CEO impersonation scams [45, 46], which often bypass technical controls by focusing on process-specific vulnerabilities as well as trust relationships within teams.

## B. Systematic Literature Review

As a starting point of our research, we asked ourselves a preliminary research question (RQ0): *“to what extent has prior research on security awareness campaigns accounted for department-specific issues in the examined organizations?”* We tackle RQ0 via a systematic literature review (SLR).

**1) Methodology:** Our SLR follows established practices: we first collect relevant papers, and then analyse them [47], in line with prior systematic reviews in security domains [48]. In what follows, we describe the systematic protocol we adopted to carry out each of these phases (carried out in Q1 2025).

- **Collection phase.** Following the guidelines by Kitchenham et al. [49] and Webster and Watson [50], we combine structured keyword-based searches with backward and forward snowballing. First, we designed two sets of query strings,<sup>2</sup> a “short” (in Listing 1) and a “long” (in Listing 2) string, which we used to search for papers (published after 2015) indexed in five popular literature databases: *ACM Digital Libraries*, *IEEE Xplore*, *Elsevier ScienceDirect*, *SpringerLink*, *Association for Information Systems (AIS)*; and we also included the proceedings of the *USENIX Security Symposium* and *NDSS Symposium* (see Appendix A).

<sup>2</sup>We centered the queries around the “cybersecurity” and “awareness” keywords. These were then paired with complementary terms such as “program”, “campaign” and “department” (including their synonyms) to refine the scope and align the search more closely with our research objectives. Due to some digital libraries returning too many irrelevant results, two separate search strings were crafted. We discuss the limitations of our search queries in §VI-B

Overall, this search yielded 1219 unique papers. Next, we manually inspected the titles and abstracts of these papers, filtering results outside our scope; for instance, we excluded papers proposing technical countermeasures (e.g., [51, 52]) or theoretical security models (e.g., [53, 54]), or literature reviews/systematizations (e.g., [55–57] or that were not related to cybersecurity (e.g., [58, 59]), or that were not in English (e.g., [60, 61]). Such a filtering process led to 21 papers being within our scope.<sup>3</sup> Then, we applied forward and backward snowballing, looking for all works that cited, or were cited by, such 21 papers (and that were within our scope); we found 6 more papers in this way. Finally, we decided to also include 2 white papers that we found by issuing the “short” string on Google, leading to 29 papers in total. All these operations have been carried out by two authors who interacted to resolve uncertainties.

- **Analysis phase.** The 29 papers have been manually analysed. The primary goal of such an analysis was to answer our preliminary RQ, which was done by assessing if the study incorporated department-specific or role-based perspectives. However, we also assessed additional aspects, such as: considered organizations, sample size, methodology, and objectives. To this purpose, we developed a codebook (which we report in the repository) through which two authors analysed each paper. We also measured the inter-code reliability: Cohen  $\kappa=0.94$ , indicating strong agreeability [63].

We report in Table I the results of coding-based analysis for each paper found in the collection phase.

```
("security" OR "cybersecurity") AND ("awareness")
AND ("program" OR "campaign") AND
("organization" OR "company" OR "department" OR
"corporation" OR "enterprise")
```

Listing 1: Short Query

```
("security" OR "cybersecurity") AND ("awareness")
AND (Abstract:("program") OR ("campaign")) AND
(Abstract:("organization") OR
Abstract:("company") OR Abstract:("department")
OR Abstract:("corporation") OR
Abstract:("enterprise"))
```

Listing 2: Long Query. Some keywords were applied only on the Abstract

**2) Results:** Let us highlight the major findings stemming from Table I, and pertaining to our preliminary RQ.

- **General vs Specific.** The wide majority (82%) of reviewed studies conceptualize cybersecurity awareness campaigns as “universal interventions” that are intended for the general employee population (e.g., [64, 65]). These campaigns typically cover topics such as phishing, password hygiene and email security. However, these studies do not consider domain-specific workflows, risk exposure or operational contexts. We note that only 5 out of 29 ( $\approx 17\%$ ) papers made an explicit reference to role- or department-specific tailoring (i.e., [66–70]). However, only a single paper [71]

<sup>3</sup>For the sake of clarity, our focus is on “papers that explicitly carried out user studies on security awareness”; by “user studies”, we mean either interviews, or user surveys, or simulations (similarly to [62]).



investigated the process of crafting targeted campaigns. However, this was done in a healthcare domain and the focus was not on departments, but employees' roles.

- *Real-world vs Proxies.* Most empirical studies ( $\approx 76\%$ ) were conducted using student populations, simulated environments or convenience samples from single organizations (e.g., [69, 72, 73]). While these designs offer controlled insights, they do not capture the complexity of real-world organizational dynamics.
- *Single vs Multi-organization.* Also, most studies ( $\approx 78\%$ ) only pertain to a single organization, making it hard to determine the extent to which any finding may hold across different organizations. For instance, Nicholson et al. [74] conducted their study within a single organization, while Alshaikh et al. [75] and Khando et al. [76] conducted research across multiple organizations.

Based on these quantitative findings, we can answer RQ0.

**ANSWER TO RQ0:** Prior work on cybersecurity awareness programs has poorly accounted for department-specific issues. Only one paper (out of 29) considered carrying out targeted campaigns—but this was done on the basis of an employee's role, and not of their department.

**3) Observations:** We enrich the findings of our SLR by making additional low-level observations. First, although some studies investigate and compare delivery formats (such as video-based [65, 68, 72, 73, 77] vs. text-based content [66, 67, 78], or microlearning [79] vs. game-based [66, 67, 80]) no paper examined whether training effectiveness varied across departments or job types. This is problematic given the increasing diversity of communication styles, workload patterns and cognitive requirements across roles. Second, even though six papers [64, 67, 71, 72, 74, 81] do make some department-specific consideration, terms such as “human resources” or “accounting” (or even “finance”) are never mentioned<sup>4</sup> in the text—indicating a lack of research that specifically focuses on these two crucial departments in modern organizations. Third, and as a disclaimer: *our SLR is not meant to invalidate prior work.* We simply point out an (arguably) crucial aspect of security-awareness programs that has been overlooked.

### C. Research Gap and Problem Statement

Our SLR highlighted that, despite the existence of dozens of papers involving, explicitly or implicitly, cybersecurity-awareness programs, limited attention has been given to department-specific issues—especially those affecting the HR and accounting departments (§II-B2).

To rectify such an oversight, we make the first step and carry out a novel user study focused specifically on these two departments of various organizations. Our study is designed to answer the following three RQ:

RQ1: *What are the specific cybersecurity threats faced by HR and accounting departments?* (§IV-A)

<sup>4</sup>These terms appear in [74], but only to specify that “support participants included receptionists and staff in accounting and HR departments.”

TABLE I: Our Classification Table

Paper	Year	Source	Type of User Study	Focus	Sample Size
Rampold et al. [71]	2024	HICSS	Survey + Interviews	Secure behavior of personnel in healthcare	8 + 12
Berens et al. [68]	2024	COSE	Field Study	Effectiveness of cybersecurity training for older adults	35
Schöni et al. [82]	2024	EuroUSEC	Field Study	Evaluation of phishing training	122
Chowdhury et al. [83]	2023	IJIS	Survey + Interviews	Cybersecurity Training for non-IT personnel	113 + 10
Gamisch and Pöhn [69]	2023	ARES	Field Study	Comparison of multiple awareness campaigns	261
Hull et al. [84]	2023	COSE	Online Study	Influence of storytelling on security behavior	339
Keshvadi et al. [85]	2023	IHTC	Survey + Training	Cybersecurity Training for non-IT personnel	208 + 12
Reeves et al. [86]	2023	COSE	Interviews + Field Study	Employee perceptions of organizational security	32
Tally et al. [87]	2023	TOCHI	Survey + Interviews	Cybersecurity perceptions of mid-career personnel	33 + 101
F. Adilia [88]	2023	ISCTE-IUL	Survey + Interviews	cybersecurity awareness campaign via Instagram	N/A
Alkhazi et al. [67]	2022	IEEE Access	Survey	Impact of awareness programs on behavior	420
Alyami et al. [80]	2022	Cyber-RCI	Survey	Success factors for SETA programs	153
Chowdhury et al. [89]	2022	COSE	Surveys	Cybersecurity training for non-IT professionals	113
Kärestad et al. [79]	2022	Future Internet	Experiment	Contextual vs. game-based phishing methods	92
Li et al. [90]	2022	CHBR	Survey	Compliance with security policies	389
H. Awaludin [91]	2022	Malmö University	Survey + Interviews	Awareness via Instagram among students	40
Abu-Amara et al. [66]	2021	INDIA Com	Pre/Field Study	Gamified cybersecurity awareness program	10
Alshaikh et al. [64]	2021	COSE	Field Study	Evaluation of existing awareness approaches	24
Reeves et al. [73]	2021	COSE	Interviews	Perceptions of security training content	26
Sterk und Heinemann [65]	2021	EICC	Field Study	Evaluation of board game for teaching security	32
Rege et al. [92]	2020	ISEC	Field Study	Social engineering training for students	N/A
Schütz and Fertig [93]	2020	HICSS	Survey	Behavior model for security compliance	204
Alshaikh et al. [75]	2018	HICSS	Interviews	Exploration of security awareness practices	18
Nicholson et al. [74]	2018	USENIX	Experiment	Security decision-making using Cybersurvival	111
Anjaria and Mishra [94]	2017	IC SoftComp	Survey	Neuroevolution adaptive training	145
Carella et al. [78]	2017	IEEE Big Data	Field Study	Effects of awareness training on phishing	753
He et al. [72]	2017	AMCIS	Experiment	Comparison of interactive training methods	228
Ki-Aries and Faily [81]	2017	COSE	Interviews	Development of persona awareness training	9
Bauer et al. [70]	2017	COSE	Interviews	Design of awareness programs for banks	33

RQ2: *What topics should cybersecurity awareness campaigns focus on to maximize their effectiveness for HR and accounting departments?* (§IV-B)

RQ3: *Which delivery methods are effective for engaging with HR and accounting employees in cybersecurity awareness campaigns?* (§IV-C)

Our RQs are inspired by the findings discussed in §II-B3. We note that such RQ are particularly valuable “today”, given that they provide novel insights pertaining to HR and accounting departments in the current cybercrime landscape.

### III. RESEARCH METHOD

To answer our research questions, we conducted semi-structured interviews (§III-A) and user surveys (§III-B). Interviews were conducted only with a case company, while surveys targeted nine different companies. Both of these were developed in agreement with the case company. Additionally, we shared our survey on a well-known professional online social network, LinkedIn, to serve as a reference point for validating the results obtained from company responses (§III-C).

#### A. Semi-structured Interviews

In the first phase of the study, we conducted semi-structured interviews with employees and managers from HR, accounting, and cybersecurity departments to explore threats, training content needs, and delivery preferences specific to each department. With this method [95], we investigated gaps and insights identified in our systematic literature review (§II-B), while also addressing emerging insights obtained during interviews.

*Design:* We defined two participant groups: (1) cybersecurity specialists and (2) HR and accounting department employees and managers. We included cybersecurity specialists to ensure technical precision in threat identification, as non-technical personnel may lack the expertise to fully recognize or articulate complex attack scenarios [37]. We developed interview guides for each target group based on Kallio et al.’s [95] five-phase approach, incorporating themes derived from a systematic literature review. Themes included tailoring awareness campaigns, training delivery methods, and behavior change. These were structured using principles from Protection Motivation Theory [96]. Following the guidance of Turner [97] and Venkatesh et al. [98], the interview guides included a warm-up phase to collect demographic and role specific information, a main section to discuss department-specific threats, training topics, delivery methods, and content relevance, targeting the needed aspects to answer the defined RQ, and a cool-down phase to facilitate open-ended reflection. Pre-tests were conducted with two representatives from each group to ensure clarity, flow, and approximate duration, following the guidelines by Helfferich [99]. A 30-minute target was established for the duration of the interview. The final interview guides contained 15 questions for cybersecurity specialists and 14 for non-technical participants (see Tables II and VIII).

*Distribution:* A total of 16 interviews were conducted (see Table III): Four were with security professionals, and twelve were with departmental employees (six each from HR and accounting). Participants were selected by purpose-sampling to ensure domain relevance, reliability, and availability, in accordance with Gläser and Laudel’s [100] criteria. All interviews were conducted remotely via Microsoft Teams during calendar weeks 7 and 8 of 2025. They were recorded with participant consent, transcribed, and anonymized for analysis.

TABLE II: Interview Guide for HR and accounting departments

ID	RQ	Category	Question
1	-	Warm-Up	What is your current role?
2	-	Warm-Up	How much experience do you have in your role at this company?
3	-	Warm-Up	How old are you?
4	1	Warm-Up	How well would you consider your knowledge of cyber security?
5	1	Topics	Have you participated in any cyber security awareness programs before?
6	2	Topics	Which topics did you find most useful or relevant?
7	2	Topics	Are there any topics you think are underrepresented in current cyber security awareness programs?
8	3	Delivery Methods	Which types of cyber security awareness materials (e.g., videos, workshops, email campaigns, games) do you find most engaging?
9	3	Delivery Methods	What changes would you suggest to make cyber security awareness campaigns more relevant and engaging for your department?
10	3	Delivery Methods	Do you think short and frequent training sessions (micro-learning) would be effective for your department?
11	2	Content	Are there particular examples or scenarios that would make cyber security training more relatable to your job responsibilities?
12	2	Content	Do you think the content of awareness campaigns should be tailored to specific roles within your department?
13	-	Cool-Down	Is there anything else you would like to add that was not covered in this interview that you think is important?
14	-	Cool-Down	Do you have a question for me?

TABLE III: Participant and Interview Characteristics

ID	Department	Age	Experience	Duration
CS1	Cyber Security	35-44	13	00:28:15
CS2	Cyber Security	25-34	2	00:28:55
CS3	Cyber Security	35-44	9	00:26:43
CS4	Cyber Security	18-24	2	00:29:07
A1	Accounting	45-54	20+	00:22:25
A2	Accounting	25-34	3	00:24:09
A3	Accounting	45-54	10+	00:24:47
A4	Accounting	45-54	12	00:29:30
A5	Accounting	25-34	4	00:25:36
A6	Accounting	45-54	16	00:28:48
HR1	Human Resources	25-34	2	00:24:21
HR2	Human Resources	25-34	1	00:42:04
HR3	Human Resources	25-34	2	00:42:04
HR4	Human Resources	25-34	8	00:30:00
HR5	Human Resources	25-34	4	00:23:56
HR6	Human Resources	45-54	20+	00:25:12

*Data Analysis:* We analyzed the transcripts using a deductive content analysis approach grounded in the methodology of Mayring [101]. Eight thematic categories were defined in advance based on findings from our systematic literature review (§II-B): (1) perception of cybersecurity awareness campaigns, (2) department-specific threats, (3) knowledge gaps and training needs, (4) delivery method preferences, (5) behavior and organizational culture, (6) barriers and challenges, (7) customization and personalization preferences, and (8) measurement and feedback mechanisms. Responses were seg-

mented into relevant themes to enable a structured comparison across departments. This allowed for the identification of shared patterns and department-specific needs. Insights gained from this analysis informed the development of a survey instrument for the next phase of the study.

### B. Company Surveys

The second phase of the study aimed to validate and extend the findings from the qualitative interviews (§III-A) by conducting a quantitative survey. This approach follows the triangulation model by Turner et al. [97] and the logic-based mixed-method framework of Venkatesh et al. [98]. The survey targeted employees and managers of HR and accounting departments.

*Design:* Unlike the interview phase, which included cybersecurity specialists, this phase exclusively focused on non-technical staff to assess their perceived risks, training preferences, and campaign relevance. This targeted sampling increased the study’s internal validity and enabled cross-sectional comparisons between departments. The development of the survey was based on the methods proposed by Döring [102] and Taherdoost [103]. The Questions were grouped into five thematic blocks: (1) demographics and context, (2) current training, (3) knowledge and threat awareness, (4) delivery method preferences, and (5) organizational culture and management support. Each block was constructed to address specific aspects of cybersecurity awareness, directly derived from the findings of previous phases. The *Demographics and Context* section includes background information about the participants, such as their department affiliation, role, and years of experience. *Current Training* section addresses the participants’ prior experience with cybersecurity training, including the training’s format, frequency, and perceived effectiveness. This information was used to determine baseline training saturation and individual experiences with existing campaigns. The majority of the survey was allocated to the *Knowledge and Threat Awareness* section that aims to evaluate employees’ knowledge of specific cybersecurity risks relevant to their role, such as phishing, invoice fraud, and social engineering. It also includes items measuring self-assessed readiness and confidence in threat detection. For this part, we used relevant topics from the HAIS-Q questionnaire as the construct has already been validated by previous research [104]. In addition, both *Current training Knowledge* and *Threat Awareness* sections were structured around the Protection Motivation Theory. Section *Delivery Method Preferences* aims to evaluate the design of customized campaigns, including preferences for training formats, delivery channels, and scheduling. *Organizational Culture and Management Support* section examined how participants perceive cybersecurity as a shared organizational responsibility. The focus was on the commitment of the management, the support of the department, and the perceived severity of the cybersecurity communication within the teams. Questions were closed-ended (yes/no, Likert scale, and ranking) to ensure reliability and enable quantitative comparisons. The survey was implemented using the GDPR-compliant Swiss platform “Findmind” (<https://en.findmind.ch/>). A pretest

with six participants confirmed the clarity of the questions and usability of the tool, and adjustments were made based on the feedback received. The final questionnaire had 36 closed-ended items and was available in English and German to improve accessibility (see Table VII).

TABLE IV: Company Characteristics and Response Participation

Company	Employees	Sector	Responses
Case Company	34,000	Manufacturing	30
1	1,000	Banking	19
2	1,300	Healthcare	14
3	500	IT	10
4	2,000	E-commerce	9
5	2,000	Industry	2
6	20	Industry	1
7	88,000	Industry	7
8	7,000	IT	1

*Distribution:* The recruitment process was multi-stage. In this case, the survey was distributed internally at the case company. Additionally, eight external organizations from sectors including banking, healthcare, and IT participated. While the primary focus was on HR and accounting departments, we also included participants from other departments within the surveyed organizations. This “Other” group serves only to better contextualize department-specific differences between HR, accounting, and other departments: including these respondents allowed us to distinguish whether observed patterns were truly specific to HR and accounting. To protect respondent anonymity, distribution was decentralized via designated company links. Data collection took place between calendar weeks 17 and 22 of 2025. A total of 93 participants completed the survey: 30 came from the case company and 63 came from external organizations. A break down of the participants of this user study is in Table IV. In terms of their role, 43 participants belong to HR, 44 to accounting, and 6 to “other” departments. More information about the demographics of our survey is provided in the Appendix C.

*Data Analysis:* We analyzed survey data using a combination of descriptive and inferential statistics, which is consistent with the best practices for quantitative analysis in mixed-methods research [105]. This approach enabled us to extend, validate and generalize the findings from the qualitative phase. First, responses from different companies were merged into a single dataset. Entries with less than 90% completion were excluded to ensure data quality. Matrix and multiple-choice responses were converted to long format, and Likert-scale items were mapped to a 1–5 numerical scale for statistical comparison. Descriptive statistics were computed to identify trends in perceptions, training engagement, and threat awareness. This included means and standard deviations for Likert items and frequency distributions for categorical variables. To assess differences between departments, a series of independent-samples t-tests were conducted to compare responses from HR and accounting participants. T-tests were applied only to Likert-scale items with sufficient coverage, which were deemed appropriate based on group size and the approximate normality of the responses. These tests evaluated whether



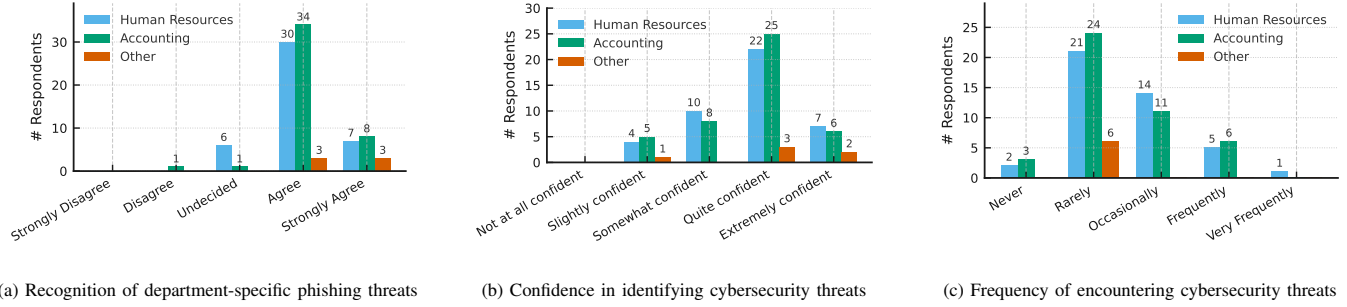


Fig. 1: Survey results comparing departments in terms of cybersecurity threat awareness. Note that,  $n=43$  for HR,  $n=44$  for accounting, and  $n=6$  for “other”.

the observed mean differences between departments were statistically significant, particularly with regard to perceived threats, training preferences, and organizational support.

### C. LinkedIn Surveys

In addition to company surveys, we also shared our survey on the LinkedIn social network, targeting once again HR and accounting personnel. The LinkedIn response group ( $n = 10$ ) served as an external reference point and control group. We used it to assess whether the insights gathered from company-affiliated participants were consistent with the responses of a more diverse and open population. To evaluate potential differences, we performed independent sample t tests to compare responses from the LinkedIn group with those from company-based participants. These comparisons allowed us to examine whether threat perception, training preferences, and attitudes toward cybersecurity awareness varied significantly between organizational and non-organizational contexts.

## IV. RESULTS

We first outline specific threats faced by HR and accounting departments, comparing them to “other” departments (§IV-A). Then, we discuss the main topics of cybersecurity awareness campaigns for these departments (§IV-B). Lastly, we detail the key delivery methods (§IV-C). These are all reported based on our mixed-methods approach that combines our qualitative semi-structured interviews with our quantitative survey. We will discuss the LinkedIn results in the next section.

### A. RQ1: Threats Faced by HR and Accounting

RQ1 focuses on elucidating the specific cybersecurity threats perceived by personnel of HR and accounting departments.

**Interviews:** The transcripts revealed clear threat patterns. Interviewees from HR consistently identified phishing attacks as the most threatening attack vector. HR interviewees specifically stressed the *phishing attempts using job applications* and *requests for employee data as a pretext*. These targeted emails aimed to exploit HR’s administrative processes, especially in recruitment, wherein large volumes of external email communication take place. Importantly, the interviews also revealed that attackers use *job application cover letters and resumes as vectors for malware delivery*, which are usually “opened” without prior thinking or considering that the file could be malicious. *Impersonation and other types of social*

*engineering attacks* were also commonly reported in the HR context. Attackers frequently attempted to *pose as company executives* by using authority and urgency to pressure HR personnel into disclosing sensitive information or processing fraudulent requests. Such attempts often occur when strict verification procedures are not applied, which leaves HR staff vulnerable to deception.

Accounting interviewees described a different threat landscape. The most frequently mentioned risks included *invoice fraud*, *credential theft* and *unauthorized access to financial systems*. Participants highlighted that attackers often *manipulate invoice templates* or *alter payment details* with the goal of redirecting funds. These attacks are typically executed during high-pressure periods such as monthly or quarterly financial closings, during which employees are under time pressure, impairing thorough verification. Credential-based threats, including *spear-phishing emails* targeting login credentials for accounting or ERP systems, were also described as becoming more sophisticated and dangerous.

A common topic in both departments was that awareness of general threats exists and it is being addressed in the existing campaigns. However, the main problem is that implementation of effective countermeasures – especially in day-to-day processes – remains problematic. This indicates that the personnel are being trained to acknowledge threats, but not how or with what to counter them. Additionally, participants stated that existing awareness campaigns rarely reflect department-specific attack vectors or scenarios. Instead, they always rely on generic examples that do not align with the operational realities and specific threats.

**Surveys:** In the survey, respondents were asked to select and rank cybersecurity threats most relevant to their work environment. Among HR participants ( $n = 43$ ), phishing attacks were stated by 91% of employees as the primary concern. This was followed by data protection risks (79%) related to handling personal information. The high percentage confirms that HR employees are aware of their exposure to attacks aimed at data exfiltration or manipulation. However, they are less informed about specific threats such as malicious QR codes, deepfake videos and supply chain attacks. This pattern is also visible in the phishing threat recognition chart (see Figure 1a), where HR employees identified phishing threats more often than accounting employees.

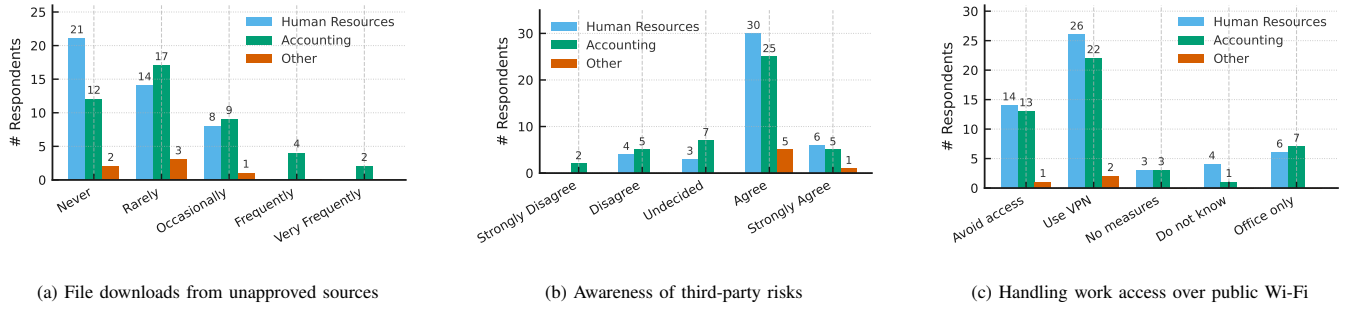


Fig. 2: Comparison of cybersecurity-related practices across departments. Note that,  $n=43$  for HR,  $n=44$  for accounting, and  $n=6$  for “other”.

For accounting respondents ( $n = 44$ ), invoice fraud emerged as the most frequently selected threat (86%), followed by credential theft (82%). These results strongly align with the qualitative insights, which identified manipulation of invoices and unauthorized access to financial systems as key concerns in the accounting domain. Moreover, 63% of accounting respondents also cited ransomware as a relevant threat, particularly in connection with the potential encryption of payment systems or accounting databases. Interestingly, as shown in the chart on confidence in identifying threats (see Figure 1b), accounting employees reported lower confidence in recognizing cybersecurity threats compared to HR. This is concerning, given their “regular” exposure to high-risk attacks.

When asked whether current training materials and awareness measures addressed department-specific risks, only 27% of the total sample agreed. Among those who disagreed, the majority came from HR and accounting, which confirms that current training lacks contextualization. The participants said the training was too general, too technical, or irrelevant to their real-world challenges. Figure 1c shows that HR and accounting employees report facing cyber threats often, as well as their dissatisfaction with the current training. This gap makes it clear that specific departments need awareness campaigns that are more customized to their workflows. Further analysis showed that this dissatisfaction was not limited to a particular level of seniority. Both staff-level employees and managers in HR and accounting indicated that the current cybersecurity training frameworks lack specificity.

**ANSWER TO RQ1:** HR and Accounting departments face distinct cybersecurity threats tied to their operational workflows. HR is most exposed to phishing and impersonation attacks exploiting hiring processes and organizational hierarchy. Accounting primarily faces invoice fraud, credential theft, and ransomware, especially during financial closings. While both departments recognize general threats, interviews and surveys reveal that current awareness efforts are too generic and fail to address department-specific risks.

### B. RQ2: Main Topics of Awareness Campaigns

The focus of RQ2 is on identifying the key cybersecurity topics that should be addressed in awareness campaigns to

effectively support the specific departmental needs.

**Interviews:** The interviews revealed that awareness campaigns must be grounded in the operational realities of each role. For HR staff, a central topic should be the secure handling of personal and sensitive employee data. Several HR participants reported uncertainty about which channels and formats are appropriate for transmitting documents such as CVs and contracts. One HR interviewee admitted: *Sometimes I send a CV by email and then I think, maybe I should have encrypted it—but it is not clear.* Another was unsure whether sharing CVs over Microsoft Teams was secure or compliant with company policies.

In accounting, the interviews pointed to a need for awareness content that addresses fraudulent financial requests and manipulation of payment processes. Interviewees described encounters with fake invoices or supplier impersonation. One interviewee stated: *“It looked exactly like the real invoice – same layout, same logo – just a different IBAN.”* To be effective, awareness campaigns should cover how to verify vendor information, authenticate requests for bank detail changes, and recognize red flags in financial documentation.

Across both departments, there was uncertainty regarding how to respond to “suspicious” situations. Several HR and accounting employees noted that they could often identify something “strange” in a message or attachment, but were unsure what to do. Hence, campaigns should clearly communicate reporting procedures and provide clarity on when an issue should be flagged, paused, or passed to security teams.

**Surveys:** The survey showed that employees share confidential files such as payroll records or contracts via email or internal messaging tools such as Teams. These methods often lack encryption or audit trails, which makes them vulnerable to man-in-the-middle or misuse attacks. This underscores the need for campaigns to cover practical guidance on secure file transfer, internal data handling policies, and the risks of casual sharing practices. In addition to file sharing, downloading behavior emerged as another weak spot (see Figure 2a). The participants acknowledged retrieving files or templates from unapproved external websites, which can expose systems to malware or data exfiltration. Training materials need to move beyond abstract warnings and instead demonstrate how malicious files are embedded in realistic formats such as fake invoices or HR templates. In accounting, where macro-enabled



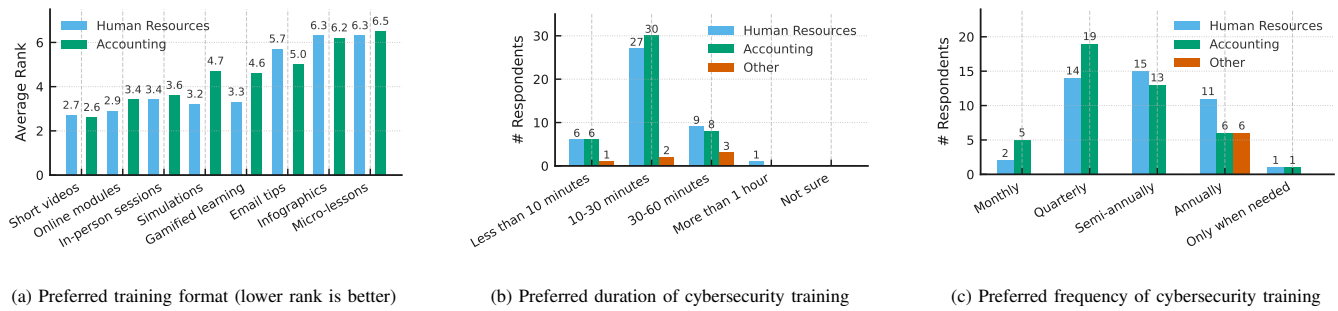


Fig. 3: Training preferences across departments. Note that,  $n=43$  for HR,  $n=44$  for accounting, and  $n=6$  for “other”.

spreadsheets or automated payment tools are common, awareness campaigns must directly address the threat of malicious documents and promote safe alternatives.

Password management also stood out as a concern. Employees admitted to reusing passwords or storing them in insecure ways. These practices place department-specific systems and tools at risk—especially those that control access to financial data or employee records. Awareness efforts should focus on promoting practical password hygiene with relatable examples. For example, showing how a reused password could compromise both the HR database and payroll systems is considered more useful than merely recommending a theoretical “strong password” rule. Finally, the survey also showed limited awareness of the cybersecurity risks tied to third-party tools (see Figure 2b) and use of public Wi-Fi (see Figure 2c). Campaigns should therefore incorporate content about shadow IT, supplier verification, and the risks of working with unapproved vendors.

**ANSWER TO RQ2:** Effective cybersecurity awareness campaigns for HR and accounting should focus on secure document handling, invoice fraud scenarios, password hygiene, and clear incident reporting procedures. Interviews emphasized the need for guidance on sharing sensitive files like CVs and contracts, and verifying financial requests. Survey data confirmed risky behaviors, including unsafe downloads, reused passwords, and uncertainty about reporting threats.

### C. RQ3: Delivery Methods

RQ3 focuses on determining which delivery methods are (perceived as being) most effective for engaging employees in cybersecurity awareness efforts.

**Interviews:** The results obtained from interviews indicate a strong and consistent preference for cybersecurity training methods that are concise, engaging, and adaptable to individual learning needs. Participants highly prefer scenario-based formats over traditional approaches dominated by static text or lengthy slide presentations. One delivery method that stood out above all others was video-based training. It is preferred for its ability to break down complex topics, present realistic and relatable scenarios, and maintain attention through clear pacing and engaging storytelling. Videos can also be revisited as needed, supporting flexible and self-paced learning. As one

interviewee explained: ... *and I think when you then do a bit of a mixture between a video and slides or you have to click again something or then say what is the right answer. I think that normally works quite well, because it is not... you are not there only passively as well.*

Accounting department participants in particular highlighted the value of hands-on, decision-driven learning. Formats such as branching scenarios or phishing simulations were favored, as they provided opportunities to apply judgment in situations that closely mirrored real-life threats. These simulations proved to be memorable and relevant, while also often reflecting the different types of fraud attempts and transactional risks. The emphasis was not just on recognizing threats but on practicing how to respond—participants mentioned traditional modules failed to deliver this aspect.

In HR, the need for customizable and time-sensitive learning was a recurring theme. HR professionals noted that their diverse responsibilities require flexibility. They appreciated training that allows them to bypass familiar content so they can spend more time on novel materials. Scenario-based learning was often mentioned, especially when it involved typical HR tasks such as handling confidential employee data or managing payroll communications.

Cybersecurity staff, meanwhile, were especially critical of conventional training formats such as long webinars or dense policy documents, which they said are often ignored or skimmed by employees. Instead, they advocated for dynamic, visually engaging materials such as short videos, interactive modules, and gamified quizzes. These formats were seen to be more efficient with modern attention spans and reflective of the fast-changing nature of cyber threats.

**Surveys:** Survey responses confirmed a strong preference for awareness campaigns that are directly relevant to employees’ day-to-day tasks. Figure 3a presents the average ranking results across departments regarding their preferred methods. Short online videos emerged as the top choice overall, especially among accounting and human resources staff. Participants appreciated these formats for their clarity, visual engagement, and ease of learning. Scenario-based simulations and interactive e-learning modules also consistently ranked in the top three, reflecting a strong inclination toward immersive and participatory formats. In contrast, more static and traditional methods, including email newsletters, infographics,

posters, and standalone microlearning sessions, ranked lower.

For training frequency and duration, employees opted for moderate and time-efficient engagement. When asked how often they would ideally participate in cybersecurity training (see Figure 3b), the most selected were quarterly ( $n = 36$ ) and semi-annually ( $n = 33$ ). Annual training sessions received moderate support ( $n = 24$ ), while monthly training ( $n = 7$ ) and ad hoc sessions ( $n = 2$ ) were the least favored. A similar pattern emerged regarding training length. Figure 3c shows that the majority of respondents ( $n = 64$ ) preferred sessions lasting between 10 and 30 minutes, with  $n = 15$  favoring ultra-short formats under 10 minutes. Only a small group supported longer sessions, with  $n = 16$  preferring 30–60 minutes and just  $n = 5$  opting for durations exceeding one hour.

The survey also explored whether employees supported the idea of skipping content they already understood. A majority of respondents ( $n = 65$ ) expressed strong support for adaptive learning, which shows a widespread desire for training formats that allow learners to focus on unfamiliar or evolving topics. Personalized experiences that respect existing knowledge and streamline the learning process were viewed as more efficient and more motivating.

**ANSWER TO RQ3:** Our user studies reveal a clear preference for concise, engaging, and job-relevant cybersecurity training. Employees across departments favored short video-based content, scenario-driven simulations, and interactive modules over static formats like email tips or policy slides. Accounting staff valued practical simulations that reflect phishing and fraud risks, while HR respondents appreciated flexible, self-paced learning tailored to their diverse responsibilities. Overall, participants preferred periodic sessions lasting no more than 30 minutes, and supported adaptive learning options that allow skipping familiar content.

## V. DISCUSSION

We draw lessons learned from our research (§V-A), position our work within related studies (§V-B), and evaluate results of industrial surveys with additional LinkedIn surveys (§V-C).

### A. Key Findings

We identify four key findings from our results.

The first key finding is that employees in both HR and accounting departments encounter cyber threats that are not only frequent but highly contextual. Our results confirm that phishing remains the dominant threat vector; however, its manifestation differs across domains. In HR, attackers often embed malware in seemingly legitimate job application materials such as CVs and cover letters, knowing these documents are often opened without technical vetting. These attack vectors exploit both human routine and process design. In contrast, accounting departments face a high prevalence of invoice fraud attempts, in which fake payment details are inserted into cloned invoice templates. These threats bypass traditional technical filters because they appear plausible in context, especially during busy periods such as month-end closings. We recommend that

future research and campaigns do more to surface and simulate these highly context-driven threats.

The second key finding is the persistent gap between reported security practices and actual behavior. Interviews revealed a strong self-perception of security awareness, wherein employees claimed to follow best practices in areas such as password use and document handling. However, survey data exposed inconsistencies: a considerable number of employees admitted to reusing passwords, sharing files via unsecured platforms, or bypassing encryption when sending sensitive data. These behaviors introduce significant risk, particularly in departments with privileged access to personal or financial records. This divergence suggests the presence of social desirability bias in qualitative self-reporting and highlights the need for behavioral validation mechanisms, such as usage telemetry or targeted simulations. However, another explanation for these inconsistencies is that the overall (perceived) security awareness of the employees that participated in the interviews (all belonging to our case company) was higher w.r.t. the employees that participated in the survey (whose respondents belong to various organizations).

The third key finding is that traditional training formats are poorly suited to fostering lasting engagement. Our data show that employees overwhelmingly prefer short, video-based content and interactive scenarios tailored to their daily tasks. Delivery formats entailing long sessions and static content, such as slide decks or newsletters, were consistently rated as least effective. The participants cited them as contributing to disengagement and information fatigue. Interestingly, content relevance was ranked as a more powerful motivator than managerial encouragement. This indicates that awareness efforts should prioritize scenario authenticity and personal applicability over hierarchical delivery or generic messaging. Future research should explore adaptive content delivery models that align training with specific job functions and user knowledge baselines.

The fourth key finding centers on the underestimated risk posed by emerging threats and the widespread demand for training personalization. Threat types such as deepfake impersonations, malicious QR codes, and supply chain intrusions were largely unfamiliar to employees, despite their increasing use in targeted attacks. In parallel, over 60% of respondents indicated a desire to skip content they already understood—suggesting that current one-size-fits-all campaigns not only fail to educate on new threats, but also waste time repeating known material. Thus, these findings call for awareness campaigns that integrate threat intelligence updates with learner autonomy. We advocate for future work on designing modular, updatable training ecosystems that adapt to evolving risks while respecting users’ existing competencies.

### B. Comparison to Prior Work

Previous studies in the domain of cybersecurity awareness, such as those by Alshaikh et al. [64], Rege et al. [92], and He et al. [72], have emphasized the importance of tailoring security training to organizational contexts and user roles. These works

focused on general role-based or sectoral adaptations but did not explore tailoring at the department level. Our findings reveal that the perceived relevance of training content varies sharply between departments within the same organization. Specifically, the results from our interviews and survey show that employees in accounting and HR are exposed to distinct threat types and expect different training formats and content. This observation extends the scope of prior work by demonstrating that department-specific tailoring is necessary to increase engagement and practical relevance.

Nicholson et al. [74] and Carella et al. [78] mentioned that training should be user-centered and participatory. However, these proposals are either theoretical or abstract. In contrast, our results identify actionable paths for participatory tailoring by embedding feedback processes at the departmental level. Interviews revealed that the absence of direct communication between campaign designers and individual departments leads to ineffective or misaligned content. Our study contributes new empirical evidence showing that tailoring efforts cannot succeed without a structured and continuous exchange between content creators and targeted department members.

Sterk and Heinemann [65], Anjaria and Mishra [94], and Schöni et al. [82] have highlighted the need to align training topics with employees' existing knowledge and operational responsibilities. However, most existing research does not provide practical guidance for selecting content that reflects department-specific tasks. Our findings address this gap. For example, HR staff expressed a need for training on handling falsified applications and protecting personal data, while accounting employees emphasized phishing, invoice fraud, and data leakage risks. The observed differences in topic preference and perceived preparedness suggest that a standardized curriculum is insufficient.

Alkhazi et al. [67], Reeves et al. [86], and Chowdhury et al. [83] have previously noted that generic training formats often fail to engage users, yet few studies have examined the role of perceived relevance as a mediating factor in campaign success. Our findings show that this perception is critical. Participants consistently reported that overly generic content lacked practical value, whereas scenario-based content rooted in their departmental context was seen as useful and memorable. This aligns with the behavioral insights discussed by Khando et al. [76], who emphasize the importance of personal and contextual alignment in changing security behavior.

### C. Verification Using LinkedIn Surveys

The LinkedIn survey group that was used as an external reference point provided us with insights regarding the applicability of the study's findings beyond the participating organizations. Although the sample size was small ( $n = 10$ ), responses were largely consistent with those from participants from companies in terms of threat perception, delivery preferences and training attitudes. The only statistically significant deviation observed through independent sample t-tests concerned the perception of emerging threats. LinkedIn respondents stated that threats

were more prominent. This may reflect heightened general awareness or differing exposure across industries.

## VI. ETHICAL CONSIDERATIONS AND LIMITATIONS

We outline the ethical precautions (§VI-A) we followed during our research, and then discuss the limitations of our work (§VI-B).

### A. Ethical Considerations

Our institutions did not have, nor required, a formal IRB process when we carried out our study. Yet, we followed established ethical guidelines throughout our research [106].

**Generic Approach:** The case company designated a contact person within the cybersecurity department to serve as the primary liaison for all coordination, approvals and communication. This individual helped us ensure that all procedures related to participant recruitment, internal communication and organizational transparency were corresponding with the company's internal policies and privacy expectations. Ethical safeguards were embedded into every stage of the research process, covering both data collection and dissemination. In addition, the study followed the university's ethical research standards and adhered to all applicable regulations on data privacy, informed consent, and participant rights. At all stages, particular care was taken to ensure that participants were treated with respect and that their privacy was protected. Moreover, our participants know our identity so they can contact us if they wish their data to be deleted.

The participation in both the qualitative and quantitative part of the study was strictly voluntary. Participants were informed about the academic nature of the research, objectives and the confidentiality of the responses. No pressure or incentives were used to influence participation, we did not use deception, and participation in our study cannot lead to any harm to our participants. For the interview phase, participants received an introductory briefing, both verbally and in writing, at the beginning of each session. They were explicitly informed that their participation was voluntary and that they could withdraw from the interview or decline to answer any question at any point, without any negative consequences. All participants gave us their informed consent prior to data collection.

No data we collected was shared with any third party—not even with the case company: this ensured that our participants were free to express their own thoughts. Indeed, we only provided a high-level summary of the findings focused on thematic insights, which could be used to improve their own cybersecurity posture, but without revealing any individual-level feedback or any raw data. This ensured that employees' participation could not be traced or evaluated internally.

**Interview Conduction:** Semi-structured interviews were conducted remotely using MS Teams (<https://microsoft.com/en-us/microsoft-teams/>). This solution ensured flexibility for participants while respecting organizational policies and schedules. Audio recording and transcription (to which participants agreed) leveraged MS Teams' built-in functions and they were stored securely on university-managed systems. The



transcripts were manually reviewed and anonymized, and all references to names, locations, or other personally identifiable information were removed. Each transcript was assigned a pseudonymous identifier to ensure traceability during analysis without compromising confidentiality.

**Survey Conduction:** The survey was carried out using “Findmind”, which is a Swiss cloud-based survey tool with servers located in Switzerland. The tool operates in compliance with European data protection regulations. Participants accessed the survey through a link distributed through email. At the beginning of the survey, participants were presented with an introductory statement that clarified the purpose of the study, confirmed the anonymity of all responses, and provided contact information for questions or concerns. The survey collected no personally-identifiable or sensitive data [107, 108].

### B. Limitations and Threats to Validity

While this research contributes actionable insights into the tailoring of department-specific cybersecurity awareness campaigns, several limitations should be acknowledged.

The literature search was executed using a defined set of academic databases and a predefined set of keywords. Thus, there is a possibility that some relevant studies may have been omitted. For instance, our primary search terms focused on the concept of “awareness”, which may have led to the exclusion of studies using adjacent or synonymous terms such as “training”, “education”, or “user engagement”. This poses a potential threat to the completeness of our SLR. To mitigate this, we employed two complementary search strings and performed both backward and forward snowballing.

Interviews were conducted within a *single multinational case company* operating in the construction sector. Although the organization provided access to critical departments, the findings are embedded within this specific organizational culture, structure and maturity level. Thus, the nature of the findings may not be directly transferable to other organizations, especially those from a different type of industry.

The coding and extraction of papers and interview transcripts were guided by a predefined data extraction sheet, which involved qualitative analysis. Hence, the overall process may be subject to *researcher bias in interpretation of findings*. We addressed this by conducting an independent review by a second researcher. Additionally, the inter-coder reliability score was calculated, which demonstrated a high agreement rate between the two coders, following a similar dual-coding approach as adopted in prior transparency studies [109].

Both phases of the study, including interviews and surveys, relied on voluntary participation. While participant recruitment aimed to ensure representation across key departments, it is possible that those more interested in or aware of cybersecurity topics were more likely to engage. This may have introduced a *self-selection bias*, potentially skewing results towards higher awareness levels or more favorable attitudes toward training. Furthermore, the *limited sample size* in the qualitative phase, while sufficient for thematic saturation, constrains the ability

to explore subgroup-specific phenomena (e.g., role seniority, geography or digital literacy).

Finally, *the empirical data collected in our study is only obtained from two departments*. However, we do not claim generalisability of our findings to other departmental units—which is an exercise we leave to future work.

## VII. CONCLUSIONS AND RECOMMENDATIONS

This study contributes the first department-specific investigation into how cybersecurity awareness campaigns are perceived and internalized by employees in HR and accounting. We show that the prevailing “one-size-fits-all” approach to training fails to account for the distinct threat landscapes, appropriate campaign structures, and topic relevance required by these critical departments. Both qualitative and quantitative results converge on the demand for short, engaging formats—especially videos and simulations—that are directly relevant to users’ actual tasks. At the same time, we reveal a widespread underestimation of emerging threats such as malicious QR codes, deepfakes, and supply chain attacks. These threats are increasingly leveraged in real-world campaigns but remain largely absent from current training materials.

Based on these findings, we recommend that cybersecurity campaign designers abandon generalized awareness strategies in favor of targeted training pathways aligned with departmental risks and responsibilities. Campaigns should reflect actual decision-making scenarios such as fraudulent payroll requests in HR or altered invoices in accounting. These should offer interactive elements that promote active learning. Adaptive modules that skip known content, clear reporting procedures, and periodic feedback loops can all help increase the effectiveness and credibility of such programs.

Looking forward, our work lays the foundation for future studies examining campaign effectiveness across additional departments, industries, and cultural settings. A promising direction is to measure the long-term behavioral impact of tailored training. For instance, this can be done through follow-up simulations or technical indicators such as secure file-sharing practices. Additionally, future research should explore the role of decentralized models of engagement, such as departmental “cyber champions”. To support this, we provide our methodological tools and data structures to encourage replication, extension, and comparative analysis by other researchers and practitioners.

## REFERENCES

- [1] B. Dupont, F. Fortin, and R. Leukfeldt, “Broadening our understanding of cybercrime and its evolution,” 2024.
- [2] J. Sikra, K. V. Renaud, and D. R. Thomas, “UK cybercrime, victims and reporting: a systematic review,” *Commonwealth Cybercrime Journal*, 2023.
- [3] Q. Cui, G.-V. Jourdan, G. V. Bochmann, I.-V. Onut, and J. Flood, “Phishing attacks modifications and evolutions,” in *European Symposium on Research in Computer Security*, 2018.
- [4] M. Bruce, J. Lusthaus, R. Kashyap, N. Phair, and F. Varese, “Mapping the global geography of cybercrime with the world cybercrime index,” *Plos One*, 2024.
- [5] “Interet crime report,” [https://www.ic3.gov/Media/PDF/AnnualReport/2024\\_IC3Report.pdf](https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf), Federal Bur. of Investigation, Tech. Rep., 2024.

- [6] "State of the phish 2024," ProofPoint, Tech. Rep., 2024, <https://www.proofpoint.com/it/resources/threat-reports/state-of-phish>.
- [7] S. Baki and R. M. Verma, "Sixteen years of phishing user studies: What have we learned?" *IEEE TDSC*, 2023.
- [8] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," *Pattern Recognition*, 2018.
- [9] R. Dhamija, J. D. Tygar, and M. Hearst, "Why phishing works," in *Proc. ACM CHI*, 2006.
- [10] "Phishing activity trends report," APWG, Tech. Rep., 2024, [https://docs.apwg.org/reports/apwg\\_trends\\_report\\_q2\\_2024.pdf](https://docs.apwg.org/reports/apwg_trends_report_q2_2024.pdf).
- [11] "Top email threats and trends," Barracuda, Tech. Rep., 2024, <https://assets.barracuda.com/assets/docs/dms/top-email-threats-and-trends-vol11.pdf>.
- [12] Slashnext, "The state of phishing," Slashnext, Tech. Rep., 2023, <https://slashnext.com/wp-content/uploads/2023/10/SlashNext-The-State-of-Phishing-Report-2023.pdf>.
- [13] "How are attackers using qr codes in phishing emails and lure documents?" Cisco Talos, Tech. Rep., 2024, <https://blog.talosintelligence.com/how-are-attackers-using-qr-codes-in-phishing-emails-and-lure-documents/>.
- [14] M. Alsharnouby, F. Alaca, and S. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," *International Journal of Human-Computer Studies*, 2015.
- [15] M. Weinz, N. Zannone, L. Allodi, and G. Apruzzese, "The Impact of Emerging Phishing Threats: Assessing Quishing and LLM-generated Phishing Emails against Organizations," in *ACM AsiaCCS*, 2025.
- [16] S. L. Schröer, N. Canevascini, I. Pekaric, P. Widmer, and P. Laskov, "The dark side of the web: Towards understanding various data sources in cyber threat intelligence," in *2025 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2025, pp. 79–89.
- [17] R. Groner, T. Witte, A. Raschke, S. Hirn, I. Pekaric, M. Frick, M. Tichy, and M. Felderer, "Model-based generation of attack-fault trees," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2023, pp. 107–120.
- [18] G. A. Akerlof and R. J. Shiller, "Phishing for phools: The economics of manipulation and deception," 2015.
- [19] T. Moore, "The economics of cybersecurity: Principles and policy options," *International Journal of Critical Infrastructure Protection*, 2010.
- [20] R. Van Wegberg, S. Tajalizadehkhoob, K. Soska, U. Akyazi, C. H. Ganan, B. Klievink, N. Christin, and M. Van Eeten, "Plug and prey? measuring the commoditization of cybercrime via online anonymous markets," in *USENIX Security Symposium*, 2018.
- [21] G. Apruzzese, H. S. Anderson, S. Dambra, D. Freeman, F. Pierazzi, and K. Roundy, "“real attackers don’t compute gradients”: bridging the gap between adversarial ml research and practice," in *IEEE conference on secure and trustworthy machine learning (SaTML)*, 2023.
- [22] D. Lain, K. Kostianen, and S. Čapkun, "Phishing in organizations: Findings from a large-scale and long-term study," in *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2022, pp. 842–859.
- [23] D. Lain, T. Jost, S. Matetic, K. Kostianen, and S. Čapkun, "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*, 2024, pp. 4182–4196.
- [24] K. Schiller, F. Adamsky, C. Eichenmüller, M. Reimert, and Z. Benenson, "Employees’ attitudes towards phishing simulations: it’s like when a child reaches onto the hot hob," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, 2024, pp. 4167–4181.
- [25] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, "Don’t click: towards an effective anti-phishing training. a comparative literature review," *Human-centric Computing and Information Sciences*, 2020.
- [26] M. L. Jensen, M. Dinger, R. T. Wright, and J. B. Thatcher, "Training to mitigate phishing attacks using mindfulness techniques," *Journal of Management Information Systems*, 2017.
- [27] R. Wash and M. M. Cooper, "Who provides phishing training? facts, stories, and people like me," in *ACM CHI*, 2018.
- [28] Z. Sun, F. B. Kokulu, P. Zhang, A. Oest, G. Stringhini, T. Bao, R. Wang, Y. Shoshitaishvili, A. Doupé, and G.-J. Ahn, "From victims to defenders: an exploration of the phishing attack reporting ecosystem," in *Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses*, 2024, pp. 49–64.
- [29] R. Burton, V. Tymchenko, N. Sundvall, M. Hoang, J. Mozley, and M. Josten, "Wordythief: A malicious spammer," in *APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, 2020, pp. 1–11.
- [30] P. Burda, A. M. Altawekji, L. Allodi, and N. Zannone, "The peculiar case of tailored phishing against smes: Detection and collective defense mechanisms at a small it company," in *2023 IEEE European symposium on security and privacy workshops (EuroS&PW)*. IEEE, 2023, pp. 232–243.
- [31] T. Meurs, M. Junger, E. Tews, and A. Abhishta, "Ransomware: How attacker’s effort, victim characteristics and context influence ransom requested, payment and financial loss," in *APWG Symposium on Electronic Crime Research (eCrime)*, 2022.
- [32] B. Dupont, "The cyber-resilience of financial institutions: significance and applicability," *Journal of cybersecurity*, 2019.
- [33] B. Acharya and P. Vadrevu, "{PhishPrint}: Evading phishing detection crawlers by prior profiling," in *USENIX Security Symposium*, 2021.
- [34] D. Timko and M. L. Rahman, "Commercial anti-smishing tools and their comparative effectiveness against modern threats," in *ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2023.
- [35] S. Vasudevan, A. Piazza, and M. Carr, "A Decade of Studies on Cyber Security Training in Organizations using Social Network Analysis: A Systematic Literature Review Through Keyword co-Occurrence Network," in *2023 International Conference on Business Analytics for Technology and Security (ICBATS)*, Mar. 2023, pp. 1–6. [Online]. Available: <https://ieeexplore.ieee.org/document/10111127>
- [36] C. Sauerwein, I. Pekaric, M. Felderer, and R. Breu, "An analysis and classification of public information security data sources used in research and practice," *Computers & security*, vol. 82, pp. 140–155, 2019.
- [37] M. Wilson, D. de Zafra, S. Pitcher, J. Tressler, and J. Ippolito, "Information Technology Security Training Requirements: a Role-and Performance-Based Model," National Institute of Standards and Technology, Gaithersburg, Tech. Rep. 800-16, 1998. [Online]. Available: <https://doi.org/10.6028/NIST.SP.800-16>
- [38] D. Hillman, Y. Harel, and E. Toch, "Evaluating organizational phishing awareness training on an enterprise scale," *Computers & Security*, 2023.
- [39] A. Darem, "Anti-phishing awareness delivery methods," *Engineering, Technology & Applied Science Research*, 2021.
- [40] T. Caldwell, "Making security awareness training work," *Computer Fraud & Security*, 2016.
- [41] I. Hwang, R. Wakefield, S. Kim, and T. Kim, "Security awareness: The first step in information security compliance behavior," *Journal of Computer Information Systems*, 2021.
- [42] Y. T. Chua, S. Parkin, M. Edwards, D. Oliveira, S. Schiffner, G. Tyson, and A. Hutchings, "Identifying unintended harms of cybersecurity countermeasures," in *APWG Symposium on Electronic Crime Research (eCrime)*, 2019.
- [43] M. Williams, "Why HR has become more of a target for cyberattacks," 2024, section: Business and Development. [Online]. Available: <https://ifamagazine.com/why-hr-has-become-more-of-a-target-for-cyberattacks/>
- [44] Oxford College of Management, "The Crucial Role of HR in Enhancing Cybersecurity," 2024. [Online]. Available: <https://www.oxfordcollegeofmanagement.com/blog/the-crucial-role-of-hr-in-enhancing-cybersecurity/>
- [45] K. Williams, "Top Cybersecurity Threats & Predictions for Accountants (2025)," 2025. [Online]. Available: <https://www.rightworks.com/blog/top-security-threats-for-accounting-firms/>
- [46] SentinelOne, "Cyber Security in Finance: Key Threats and Strategies," 2025. [Online]. Available: <https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-in-finance/>
- [47] M. L. Rethlefsen, S. Kirtley, S. Waffenschmidt, A. P. Ayala, D. Moher, M. J. Page, and J. B. Koffel, "Prisma-s: an extension to the prisma statement for reporting literature searches in systematic reviews," *Systematic reviews*, 2021.
- [48] I. Pekaric, R. Groner, T. Witte, J. G. Adigun, A. Raschke, M. Felderer, and M. Tichy, "A systematic review on security and safety of self-adaptive systems," *Journal of Systems and Software*, p. 111716, 2023.
- [49] B. A. Kitchenham, D. Budgen, and P. Brereton, *Evidence-based software engineering and systematic reviews*. CRC press, 2015.
- [50] J. Webster and R. T. Watson, "Analyzing the past to prepare for the future: Writing a literature review," *MIS quarterly*, pp. xiii–xxiii, 2002.
- [51] N. Humaidi and S. H. A. Alghazo, "Procedural information security

- countermeasure awareness and cybersecurity protection motivation in enhancing employee's cybersecurity protective behaviour," in *2022 10th International Symposium on Digital Forensics and Security (IS-DFS)*. IEEE, 2022, pp. 1–10.
- [52] S. Hart, A. Margheri, F. Paci, and V. Sassone, "Riskio: A serious game for cyber security awareness and education," *Computers & Security*, vol. 95, p. 101827, 2020.
- [53] N. S. Safa and R. Von Solms, "An information security knowledge sharing model in organizations," *Computers in Human Behavior*, vol. 57, pp. 442–451, 2016.
- [54] N. S. Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Computers & security*, vol. 56, pp. 70–82, 2016.
- [55] D. Jampen, G. Gür, T. Sutter, and B. Tellenbach, "Don't click: towards an effective anti-phishing training. A comparative literature review," *Human-centric Computing and Information Sciences*, vol. 10, no. 1, p. 33, Aug. 2020. [Online]. Available: <https://doi.org/10.1186/s13673-020-00237-7>
- [56] K. H. Sharif and S. Y. Ameen, "A Review of Security Awareness Approaches With Special Emphasis on Gamification," in *2020 International Conference on Advanced Science and Engineering (ICOASE)*, Dec. 2020, pp. 151–156. [Online]. Available: <https://ieeexplore.ieee.org/document/9436595>
- [57] O. Pahlavanpour and S. Gao, "A systematic mapping study on gamification within information security awareness programs," *Heliyon*, vol. 10, no. 19, p. e38474, Oct. 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2405844024145057>
- [58] A. A. Barreda, A. Bilgihan, K. Nusair, and F. Okumus, "Generating brand awareness in online social networks," *Computers in human behavior*, vol. 50, pp. 600–609, 2015.
- [59] A. Dabbous and K. A. Barakat, "Bridging the online offline gap: Assessing the impact of brands' social network content quality on brand awareness and purchase intention," *Journal of retailing and consumer services*, vol. 53, p. 101966, 2020.
- [60] J. P. C. Mendoza, "Concientización en ciberseguridad a través de ataques de ingeniería social," *INF-FCPN-PGI Revista PGI*, pp. 62–64, 2020.
- [61] A. Infante-Moro, J. C. Infante-Moro, and J. Gallardo-Pérez, "Factores claves para concienciar la ciberseguridad en los empleados," *Revista de pensamiento estratégico y seguridad CISDE*, vol. 7, no. 1, pp. 69–79, 2022.
- [62] I. Pekaric and G. Apruzzese, "'We provide our resources in a dedicated repository': Surveying the Transparency of HICSS Publications," in *HICSS*, 2025.
- [63] M. J. Warrens, "Five ways to look at cohen's kappa," *Journal of Psychology & Psychotherapy*, 2015.
- [64] M. Alshaikh, S. B. Maynard, and A. Ahmad, "Applying social marketing to evaluate current security education training and awareness programs in organisations," *Computers & Security*, vol. 100, p. 102090, Jan. 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404820303631>
- [65] F. Sterk and A. Heinemann, "It is not as simple as that: Playing out password security trainings in order to nudge password changes," in *Proceedings of the 2021 European Interdisciplinary Cybersecurity Conference*, ser. EICC '21. New York, NY, USA: Association for Computing Machinery, Nov. 2021, pp. 20–25. [Online]. Available: <https://dl.acm.org/doi/10.1145/3487405.3487653>
- [66] F. Abu-Amara and H. Tamimi, "Cyber Shield Security Awareness Program," in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, Mar. 2021, pp. 422–425. [Online]. Available: <https://ieeexplore.ieee.org/document/9441148>
- [67] B. Alkhazi, M. Alshaikh, S. Alkhezi, and H. Labbaci, "Assessment of the Impact of Information Security Awareness Training Methods on Knowledge, Attitude, and Behavior," *IEEE Access*, vol. 10, pp. 132 132–132 143, 2022, conference Name: IEEE Access. [Online]. Available: <https://ieeexplore.ieee.org/document/9991148>
- [68] B. M. Berens, M. Mossano, and M. Volkamer, "Taking 5 minutes protects you for 5 months: Evaluating an anti-phishing awareness video," *Computers & Security*, vol. 137, p. 103620, Feb. 2024. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404823005308>
- [69] L. Gamisch and D. Pöhn, "A study of different awareness campaigns in a company," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023, pp. 1–8.
- [70] S. Bauer, E. W. N. Bernroider, and K. Chudzikowski, "Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks," *Computers & Security*, vol. 68, pp. 145–159, Jul. 2017. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404817300871>
- [71] F. Rampold, J. Heinsohn, F. Schütz, J. Klein, T. Keller, K. Masuch, and J. Warwas, "Custom Solutions for Diverse Needs: Laying the Foundation for Tailored SETA Programs in the Healthcare Domain," *Hawaii International Conference on System Sciences 2024 (HICSS-57)*, Jan. 2024. [Online]. Available: [https://aisel.aisnet.org/hicss-57/hc/security\\_and\\_privacy/2](https://aisel.aisnet.org/hicss-57/hc/security_and_privacy/2)
- [72] W. He, M. Anwar, L. Li, X. Yuan, I. Ash, and L. Xu, "Effects of Different Evidence-based Cybersecurity Training Methods on Employees," *AMCIS 2017 Proceedings*, Aug. 2017. [Online]. Available: <https://aisel.aisnet.org/amcis2017/TREOs/Presentations/22>
- [73] A. Reeves, D. Calic, and P. Delfabbro, "'Get a red-hot poker and open up my eyes, it's so boring'": Employee perceptions of cybersecurity training," *Computers & Security*, vol. 106, p. 102281, Jul. 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S016740482100105X>
- [74] J. Nicholson, L. Coventry, and P. Briggs, "Introducing the Cybersurvival Task: Assessing and Addressing Staff Beliefs about Effective Cyber Protection," 2018, pp. 443–457. [Online]. Available: <https://www.usenix.org/conference/soups2018/presentation/nicholson>
- [75] M. Alshaikh, S. B. Maynard, A. Ahmad, and S. Chang, "An Exploratory Study of Current Information Security Training and Awareness Practices in Organizations," *Hawaii International Conference on System Sciences 2018 (HICSS-51)*, Jan. 2018. [Online]. Available: [https://aisel.aisnet.org/hicss-51/os/practice-based\\_research/4](https://aisel.aisnet.org/hicss-51/os/practice-based_research/4)
- [76] K. Khando, S. Gao, S. M. Islam, and A. Salman, "Enhancing employees information security awareness in private and public organisations: A systematic literature review," *Computers & Security*, vol. 106, p. 102267, Jul. 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404821000912>
- [77] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237–248, Mar. 2014, publisher: Taylor & Francis \_eprint: <https://doi.org/10.1080/0144929X.2012.708787>. [Online]. Available: <https://doi.org/10.1080/0144929X.2012.708787>
- [78] A. Carella, M. Kotsoev, and T. M. Truta, "Impact of security awareness training on phishing click-through rates," in *2017 IEEE International Conference on Big Data (Big Data)*, Dec. 2017, pp. 4458–4466. [Online]. Available: <https://ieeexplore.ieee.org/document/8258485>
- [79] J. Kävrestad, A. Hagberg, M. Nohlberg, J. Rambusch, R. Roos, and S. Furnell, "Evaluation of Contextual and Game-Based Training for Phishing Detection," *Future Internet*, vol. 14, no. 4, p. 104, Apr. 2022, number: 4 Publisher: Multidisciplinary Digital Publishing Institute. [Online]. Available: <https://www.mdpi.com/1999-5903/14/4/104>
- [80] A. Alyami, D. Sammon, K. Neville, and C. Mahony, "The Critical Success Factors for Security Education, Training and Awareness (SETA) Programmes," in *2022 Cyber Research Conference - Ireland (Cyber-RCI)*, Apr. 2022, pp. 1–12. [Online]. Available: <https://ieeexplore.ieee.org/document/10032674>
- [81] D. Ki-Aries and S. Faily, "Persona-centred information security awareness," *Computers & Security*, vol. 70, pp. 663–674, Sep. 2017. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404817301566>
- [82] L. Schöni, V. Carles, M. Strohmeier, P. Mayer, and V. Zimmermann, "You Know What? - Evaluation of a Personalised Phishing Training Based on Users' Phishing Knowledge and Detection Skills," in *Proceedings of the 2024 European Symposium on Usable Security*, ser. EuroUSEC '24. New York, NY, USA: Association for Computing Machinery, Nov. 2024, pp. 1–14. [Online]. Available: <https://dl.acm.org/doi/10.1145/3688459.3688460>
- [83] N. Chowdhury and V. Gkioulos, "A personalized learning theory-based cyber-security training exercise," *International Journal of Information Security*, vol. 22, no. 6, pp. 1531–1546, Dec. 2023. [Online]. Available: <https://doi.org/10.1007/s10207-023-00704-z>
- [84] D. M. Hull, S. W. Schuetz, and P. B. Lowry, "Tell me a story: The effects that narratives exert on meaningful-engagement outcomes in antiphishing training," *Computers & Security*, vol. 129, p. 103252, Jun. 2023. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404823001621>



- [85] S. Keshvadi, "Enhancing Western Organizational Cybersecurity Resilience through Tailored Education for Non-Technical Employees," in *2023 IEEE International Humanitarian Technology Conference (IHTC)*, Nov. 2023, pp. 1–6, iSSN: 2837-4800. [Online]. Available: <https://ieeexplore.ieee.org/document/10508824>
- [86] A. Reeves, D. Calic, and P. Delfabbro, "Generic and unusable": Understanding employee perceptions of cybersecurity training and measuring advice fatigue," *Computers & Security*, vol. 128, p. 103137, May 2023. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404823000470>
- [87] A. C. Tally, J. Abbott, A. Bochner, S. Das, and C. Nippert-Eng, "What Mid-Career Professionals Think, Know, and Feel About Phishing: Opportunities for University IT Departments to Better Empower Employees in Their Anti-Phishing Decisions," *Proc. ACM Hum.-Comput. Interact.*, vol. 7, no. CSCW1, pp. 113:1–113:27, Apr. 2023. [Online]. Available: <https://dl.acm.org/doi/10.1145/3579547>
- [88] F. Adilia, "Raising cybersecurity awareness of telecommunication company employee through instagram campaign: Case study: Pt media telekomunikasi mandiri," Master's thesis, ISCTE-IUL, 2023, supervisor: Carlos José Corredoura Serrão.
- [89] N. Chowdhury, S. Katsikas, and V. Gkioulos, "Modeling effective cybersecurity training frameworks: A delphi method-based study," *Computers & Security*, vol. 113, p. 102551, Feb. 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404821003758>
- [90] L. Li, L. Xu, and W. He, "The effects of antecedents and mediating factors on cybersecurity protection behavior," *Computers in Human Behavior Reports*, vol. 5, p. 100165, Mar. 2022. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2451958821001135>
- [91] H. M. Awaludin, "Raising cyber security awareness using social media: Case study of security campaign on instagram," 2022, faculty of Technology and Society.
- [92] A. Rege, T. Nguyen, and R. Bleiman, "A social engineering awareness and training workshop for STEM students and practitioners," in *2020 IEEE Integrated STEM Education Conference (ISEC)*, Aug. 2020, pp. 1–6, iSSN: 2330-331X. [Online]. Available: <https://ieeexplore.ieee.org/document/9280596>
- [93] A. Schütz, K. Weber, and T. Fertig, "Analyze Before You Sensitize: Preparation of a Targeted ISA Training," *Hawaii International Conference on System Sciences 2020 (HICSS-53)*, Jan. 2020. [Online]. Available: [https://aisel.aisnet.org/hicss-53/st/security\\_and\\_privacy\\_of\\_hci/4](https://aisel.aisnet.org/hicss-53/st/security_and_privacy_of_hci/4)
- [94] K. Anjaria and A. Mishra, "Neuroevolution for effective information security training," in *2017 International Conference on Soft Computing and its Engineering Applications (icSoftComp)*, Dec. 2017, pp. 1–6. [Online]. Available: <https://ieeexplore.ieee.org/document/8280078>
- [95] H. Kallio, A.-M. Pietilä, M. Johnson, and M. Kangasniemi, "Systematic methodological review: developing a framework for a qualitative semi-structured interview guide," *Journal of Advanced Nursing*, vol. 72, no. 12, pp. 2954–2965, 2016, eprint: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/jan.13031>. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1111/jan.13031>
- [96] H. Boer and E. R. Seydel, "Protection motivation theory," in *Predicting health behaviour: Research and practice with social cognition models*. eds. Mark Conner, Paul Norman. Open University Press, 1996, pp. 95–120.
- [97] S. F. Turner, L. B. Cardinal, and R. M. Burton, "Research Design for Mixed Methods: A Triangulation-based Framework and Roadmap," *Organizational Research Methods*, vol. 20, no. 2, pp. 243–267, Apr. 2017, publisher: SAGE Publications Inc. [Online]. Available: <https://doi.org/10.1177/1094428115610808>
- [98] V. Venkatesh, S. A. Brown, and H. Bala, "Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems," *MIS Quarterly*, vol. 37, no. 1, pp. 21–54, 2013, publisher: Management Information Systems Research Center, University of Minnesota. [Online]. Available: <https://www.jstor.org/stable/43825936>
- [99] C. Helfferich, "Leitfaden- und Experteninterviews," in *Handbuch Methoden der empirischen Sozialforschung*, N. Baur and J. Blasius, Eds. Wiesbaden: Springer Fachmedien, 2019, pp. 669–686. [Online]. Available: [https://doi.org/10.1007/978-3-658-21308-4\\_44](https://doi.org/10.1007/978-3-658-21308-4_44)
- [100] J. Gläser and G. Laudel, *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen*, 3rd ed., ser. Lehrbuch. Wiesbaden: VS Verlag für Sozialwissenschaften, 2009.
- [101] P. Mayring, "Qualitative Inhaltsanalyse," in *Handbuch Qualitative Forschung in der Psychologie*, G. Mey and K. Mruck, Eds. Wiesbaden: VS Verlag für Sozialwissenschaften, 2010, pp. 601–613. [Online]. Available: [https://doi.org/10.1007/978-3-531-92052-8\\_42](https://doi.org/10.1007/978-3-531-92052-8_42)
- [102] N. Döring, *Forschungsmethoden und Evaluation in den Sozial- und Humanwissenschaften*. Berlin, Heidelberg: Springer, 2023. [Online]. Available: <https://link.springer.com/10.1007/978-3-662-64762-2>
- [103] H. Taherdoost, "Data Collection Methods and Tools for Research; A Step-by-Step Guide to Choose Data Collection Technique for Academic and Business Research Projects," *International Journal of Academic Research in Management (IJARM)*, vol. 10, no. 38, Jun. 2021. [Online]. Available: <https://hal.science/hal-03741847/document>
- [104] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The human aspects of information security questionnaire (hais-q): Two further validation studies," *Computers & Security*, vol. 66, pp. 40–51, 2017. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0167404817300081>
- [105] A. C. Klassen, J. Creswell, V. L. Plano Clark, K. C. Smith, and H. I. Meissner, "Best practices in mixed methods for quality of life research," *Quality of life Research*, vol. 21, no. 3, pp. 377–380, 2012.
- [106] M. Bailey, D. Dittrich, E. Kenneally, and D. Maughan, "The menlo report," *IEEE Security & Privacy*, vol. 10, no. 2, pp. 71–75, 2012.
- [107] E. Commission, "Sensitive data," [https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data_en).
- [108] U. D. of the Treasury, "Sensitive personal data," <https://home.treasury.gov/taxonomy/term/7651>.
- [109] I. Pekaric and G. Apruzzese, "We provide our resources in a dedicated repository": Surveying the Transparency of HICSS publications," in *Proc. Hawaii International Conference on System Sciences (HICSS)*, 2025.

## APPENDIX

### A. Systematic Literature Review

Tables V and VI summarize the search outcomes across different sources and detail the number of papers included at each phase of the selection process as part of the systematic literature review.

TABLE V: Search Results and Inclusion Details

Source	Search String	Search Results	Included
ACM DL	Long	99	2
IEEE Xplore	Short	361	8
USENIX	Short	1	1
NDSS	Short	0	0
ScienceDirect	Short	115	4
Springer	Long	175	1
AIS	Long	468	3
<b>Total</b>		1219	21

TABLE VI: Number of included papers by search phase

Phase	Number of included papers
Keyword Search	21
Backward Search	2
Forward Search	4
White Literature	2
<b>Total</b>	29

### B. Interview and Survey Guides

Table VII presents the questions as well as possible answers from the company survey. In addition, in Table II, we provide the interview guide with all the questions targeting cybersecurity specialists.

TABLE VII: Survey Questions and Answers

ID	RQ	Category	Question English	Answers
1	-	Demographics and Context	What department do you currently work in?	HR, Finance, Other
2	-	Demographics and Context	What is your role within your department?	Employee, Team Lead, Manager, Director (or above)
3	-	Demographics and Context	How long have you worked in your current role?	Less than 1 year, 1-3 years, 4-7 years, 8-10 years, More than 10 years
4	-	Demographics and Context	How old are you (age category)?	18-24, 25-34, 35-44, 45-54, 55-65
5	3	Current Training	How often do you currently receive cybersecurity awareness training (e.g. online courses, workshops)?	Monthly, Quarterly, Twice per year, Once per year, I don't recall receiving any
6	3	Current Training	How long does your typical cybersecurity training session last currently?	Less than 10 minutes, 10-30 minutes, 30-60 minutes, More than 1 hour, Not sure
7	3	Current Training	The current cybersecurity training format matches how I learn best.	Likert
8	2	Current Training	I have changed how I handle emails/files due to past cybersecurity training.	Likert
9	1	Knowledge and Threat Awareness	I believe my department is more targeted than others when it comes to cybersecurity threats.	Likert
10	2	Knowledge and Threat Awareness	How relevant do you currently find cybersecurity awareness materials provided by your organization (to my department's daily tasks)?	Likert
11	1	Knowledge and Threat Awareness	The cybersecurity training I receive helps me feel confident in spotting and responding to threats.	Likert
12	2	Knowledge and Threat Awareness	How confident are you in identifying cybersecurity threats that are specific to your department (e.g., payroll scams, invoice fraud)?	Likert
13	2	Knowledge and Threat Awareness	I can recognize threats such as phishing emails targeting my departments activities (e.g., fake payroll or invoice requests).	Likert
14	1	Knowledge and Threat Awareness	How often do you encounter cybersecurity threats (e.g., phishing attempts)?	Never, Rarely, Occasionally, Frequently, Very Frequently
15	2	Knowledge and Threat Awareness	I am aware of the risks associated with third-party platforms/tools we use.	Likert
16	2	Knowledge and Threat Awareness	How often do you download files or templates from websites not provided by IT or your team?	Never, Rarely, Occasionally, Frequently, Very Frequently
17	2	Knowledge and Threat Awareness	When setting a password for a work-related account, which of the following do you typically consider?	Length, Symbols, Reuse, Remembering ease, System-generated
18	2	Knowledge and Threat Awareness	Which of these statements best describes how you manage your work passwords?	Reuse same, Vary slightly, Different for each, Use password manager
19	2	Knowledge and Threat Awareness	When using a public Wi-Fi (e.g., airport or café) how do you handle work-related access?	Avoid, Use VPN, Use without measures, Don't know, Never work outside
20	2	Knowledge and Threat Awareness	I know what steps to take after a suspected cyber security breach.	Likert
21	2	Knowledge and Threat Awareness	Do you know how to report a cyber security incident within your organization?	Likert
22	2	Knowledge and Threat Awareness	I know the correct steps to securely store sensitive work-related documents/data.	Likert
23	2	Knowledge and Threat Awareness	How do you usually share confidential files (e.g., payroll, contract data) with colleagues or vendors?	Secure internal tools, Regular email, Cloud services, Not sure
24	2	Knowledge and Threat Awareness	Cyber security training at my company addresses newly emerging threats in a timely manner.	Likert
25a	2	Knowledge and Threat Awareness	I am familiar with ... deepfake videos as a cybersecurity threat.	Yes/No
25b	2	Knowledge and Threat Awareness	I am familiar with ... malicious QR codes as a cybersecurity threat.	Yes/No
25c	2	Knowledge and Threat Awareness	I am familiar with ... supply chain cyber attacks.	Yes/No
25d	2	Knowledge and Threat Awareness	I am familiar with ... phishing via messaging apps or social media.	Yes/No
26	3	Delivery Method Preferences	I feel comfortable asking questions or making mistakes during cybersecurity training.	Likert
27	3	Delivery Method Preferences	I prefer cybersecurity awareness campaigns that use realistic scenarios based on my daily tasks.	Likert
28	3	Delivery Method Preferences	What would motivate you most to actively participate in cybersecurity training?	Relevance to tasks, Engaging content, Incentives, Manager encouragement
29	3	Delivery Method Preferences	Rank the following training formats in order of your preference (1 = most preferred):	Videos, Interactive modules, In-person sessions, Simulations, Games, Newsletters, Infographics, Micro-learning
30	3	Delivery Method Preferences	How frequently would you prefer cybersecurity training to occur to maintain awareness effectively?	Monthly, Quarterly, Semi-annually, Annually, Only when needed
31	3	Delivery Method Preferences	Based on your selected training frequency, how long should one cybersecurity training session last?	Less than 10 min, 10-30 min, 30-60 min, More than 1 hour, Not sure
32	3	Delivery Method Preferences	I would like the ability to skip parts of the training I already know.	Likert
33	3	Organizational Culture and Management Support	My team head/manager/director reinforces cybersecurity best practices in our team.	Likert
34	1	Organizational Culture and Management Support	In your opinion, how seriously does your organization take cybersecurity?	Likert
35	1	Organizational Culture and Management Support	Cybersecurity is discussed regularly within my department (e.g., in team meetings or chats).	Likert
36	1	Organizational Culture and Management Support	I feel cybersecurity is mainly the responsibility of the IT department and not part of my daily work experience.	Likert

TABLE VIII: Interview guide for cybersecurity specialists

ID	RQ	Category	Question
1	-	Warm-Up	What is your current role?
2	-	Warm-Up	How many years of experience do you have in your role?
3	-	Warm-Up	How old are you?
4	-	Warm-Up	What topics are you working on the most?
5	1	General	Based on your expertise, what are the most common cybersecurity threats faced by organizations?
6	1	General	What role do human errors play in cybersecurity risks?
7	1	HR	What are the top three cybersecurity risks associated with HR departments?
8	1	HR	How do cyber criminals typically exploit vulnerabilities in HR departments?
9	1	Finance	What are the top three cybersecurity risks associated with Finance departments?
10	1	Finance	How do cyber criminals typically exploit vulnerabilities in Finance departments?
11	2	Recommendations	What preventative measures do you recommend for addressing department-specific cybersecurity threats?
12	2	Recommendations	What topics should be covered in the awareness campaigns for the departments?
13	3	Recommendations	What delivery method would you think is engaging for the departments?
14	-	Cool-Down	Is there anything else you would like to add that was not covered in this interview that you think is important?
15	-	Cool-Down	Do you have a question for me?

### C. Survey Demographics

In the following, we provide an overview of the demographics of the participants from the company survey. Table IX showcases the role distribution; Table X highlights the tenure of department affiliation; and Table XI visualizes the age distribution of the participants.

Table IX categorizes participants by their job roles and department. The majority of respondents in both the HR and Accounting departments were employees (30 and 34, respectively), followed by team leads, managers, and directors. Accounting had slightly higher representation in senior roles, including directors ( $n = 3$ ), than HR ( $n = 1$ ). All participants in the "Other" category identified as employees.

TABLE IX: Role Distribution by Department

Role	HR	Accounting	Other
Employee	30	34	6
Team Lead	8	4	0
Manager	4	3	0
Director (or above)	1	3	0

Table X details participants' length of service at their current role, categorized by department. Most respondents had between one and seven years of experience. Notably, the accounting department had a higher number of participants in

the "more than ten years" category ( $n = 12$ ). HR participants were more evenly distributed across the lower tenure brackets. Minimal responses were recorded for the "Other" category. Table XI shows the age ranges of participants by department. The largest age group overall was 35–44, followed by 45–54. HR had a broader age distribution, while accounting was more concentrated in the 45–54 age range. Participants aged 18–24 were minimally represented in all groups.

TABLE X: Tenure Distribution by Department

Tenure	HR	Accounting	Other
Less than 1 year	5	9	0
1-3 years	17	14	0
4-7 years	12	6	2
8-10 years	6	3	1
More than 10 years	3	12	3

TABLE XI: Age Distribution by Department

Age	HR	Accounting	Other
18–24 years	1	3	0
25–34 years	9	7	0
35–44 years	17	14	3
45–54 years	13	18	1
55–65 years	3	2	2