

DEPARTMENT-SPECIFIC SECURITY AWARENESS CAMPAIGNS: A CROSS-ORGANIZATIONAL STUDY OF HR AND ACCOUNTING

ECRIME 2025

Matthias Pfister, Giovanni Apruzzese
and Irdin Pekaric



THE PROBLEM: CYBERSECURITY AWARENESS CAMPAIGNS ARE BROKEN

- Organizations invest heavily in technical countermeasures, yet attackers still exploit human behavior
- Awareness campaigns - often generic, repetitive, and not aligned with actual departmental realities
- “Machine-based” defenses can be evaded; people remain the decisive factor
- “Awareness ≠ education ≠ training, but awareness underpins both

**DON'T CLICK
THAT LINK!**



**BEWARE OF PHISHING EMAILS
REPORT ANY SUSPICIOUS ACTIVITY**



Systematic
Literature Review



Semi-Structured
Interviews



Surveys



Strategies



METHOD



SYSTEMATIC LITERATURE REVIEW (1)



RQ0: “To what extent has prior research on security awareness campaigns accounted for department-specific issues in examined organizations?”

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
Total		1219	21



Answer: Prior work has poorly accounted for department-specific aspects; only five studies mentioned departmental tailoring, none analyzed it empirically.



SYSTEMATIC LITERATURE REVIEW (1)

- ◆ 82 % of reviewed studies treated awareness campaigns as “one-size-fits-all.”
- ◆ 76 % relied on student or single-organization convenience samples.
- ◆ Only 5 out of 29 studies mentioned any department- or role-specific tailoring.
- ◆ Only one actually attempted targeted campaigns — and that was limited to healthcare roles, not organizational departments.
- ◆ **Conclusion: The field overlooks context, workflow, and communication diversity within organizations.**



RESEARCH QUESTIONS



RQ1: What cybersecurity threats are most relevant to HR and Accounting departments?



RQ2: What are the main themes and topics addressed in existing security awareness campaigns across departments?



RQ3: How do departments differ in their preferred delivery formats and communication styles for awareness materials?



INTERVIEWS

- ◆ Sample: 16 participants from Accounting, HR and Cybersecurity departments
- ◆ Predefined eight thematic categories derived from SLR findings:
 1. Perception of 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
 8. Measurement and feedback mechanisms
- ◆ Transcripts segmented per theme, enabling cross-department comparisons.



SURVEYS

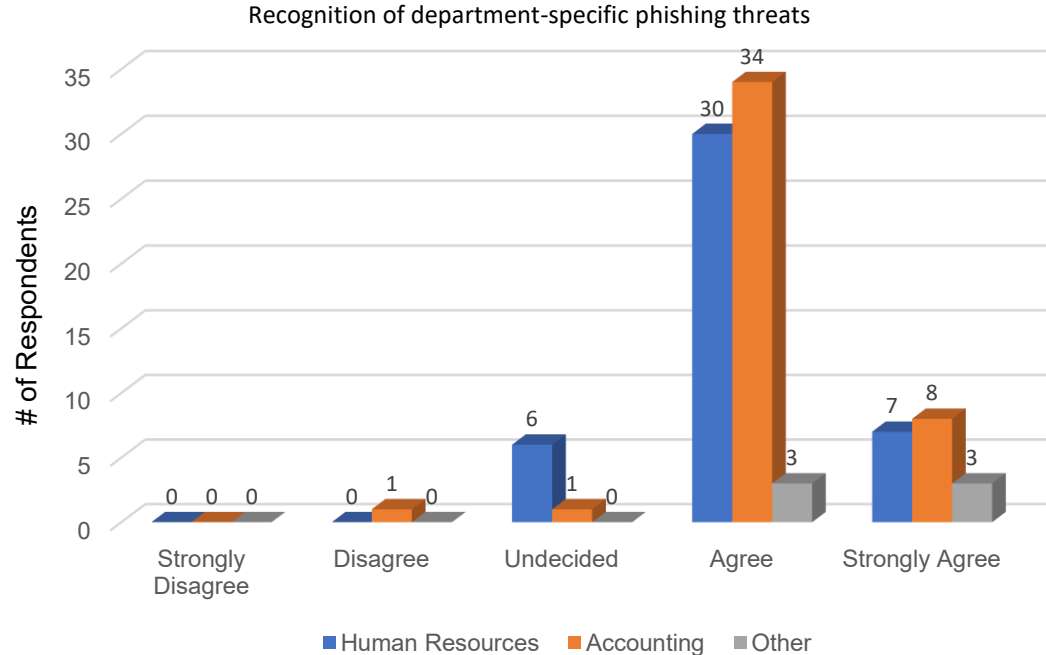
- Sample: Non-technical employees and managers from HR and Accounting departments (n = 93 + 10)
- Hosted on GDPR-compliant Findmind platform.
- Five thematic blocks:
 - Demographics & Context: department, role, experience.
 - Current Training: formats, frequency, and perceived effectiveness.
 - Knowledge & Threat Awareness: phishing, invoice fraud, social engineering.
 - Delivery Preferences: favored media, scheduling, and length.
 - Organizational Culture: management commitment and peer perception.



FINDINGS RQ1

HR participants identified phishing as the most frequent and threatening vector.

- Attackers disguise malicious attachments in job applications, CVs, and cover letters.
- Social engineering and executive impersonation used to pressure HR staff into disclosing sensitive data



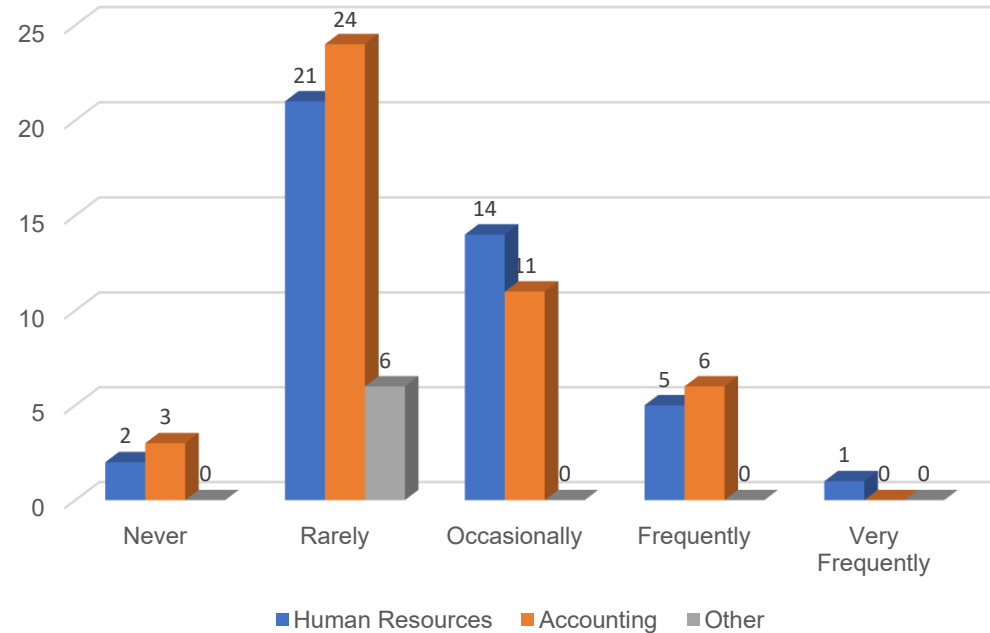
FINDINGS RQ1

Accounting faced invoice fraud, credential theft, and unauthorized access to financial systems.

- Fraudulent invoice templates and altered payment details.

Both departments receive generic training that acknowledges threats but rarely covers department-specific countermeasures.

Frequency of encountering cybersecurity threats

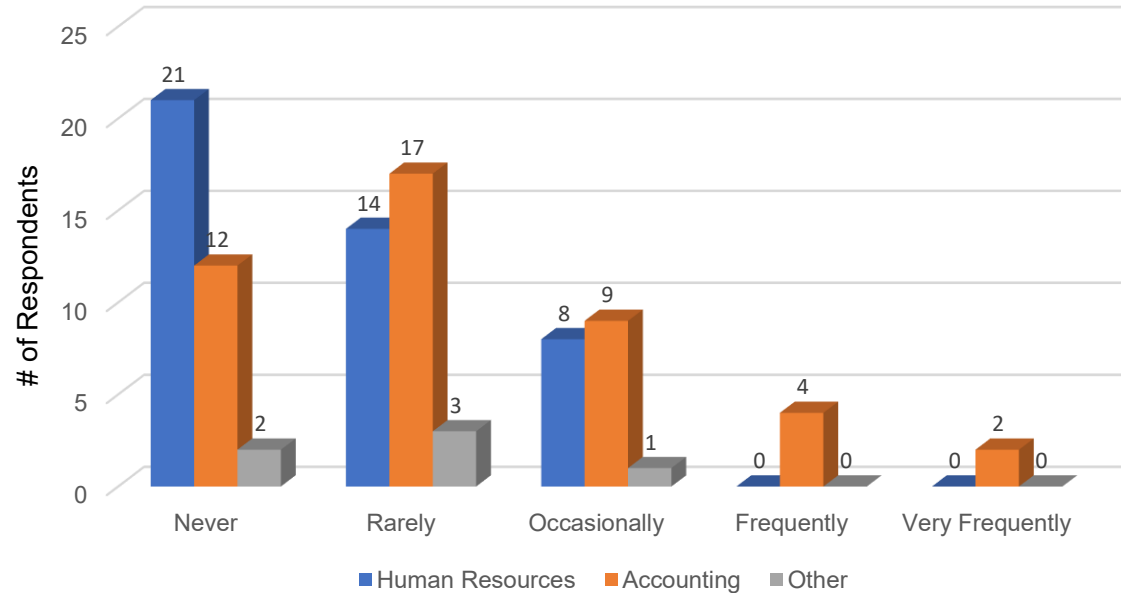


FINDINGS RQ2

Existing campaigns emphasize phishing, password hygiene, and general data protection, but ignore context-specific scenarios (e.g., HR recruitment workflows, Accounting payment approvals).

Awareness materials are outdated and repetitive

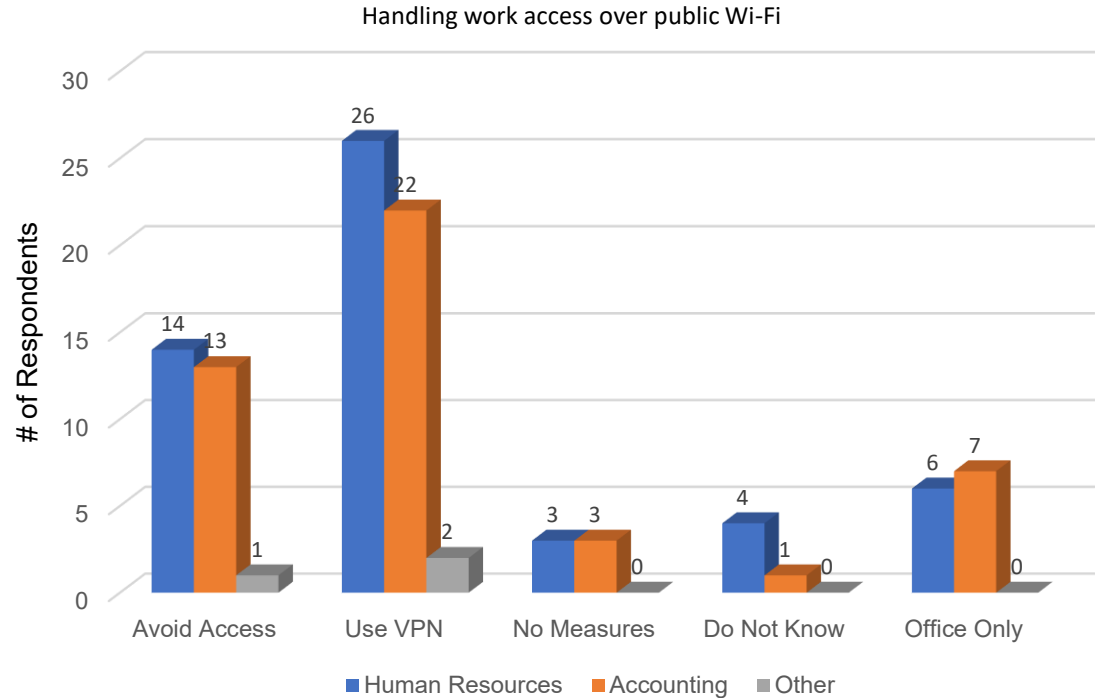
File downloads from unapproved sources



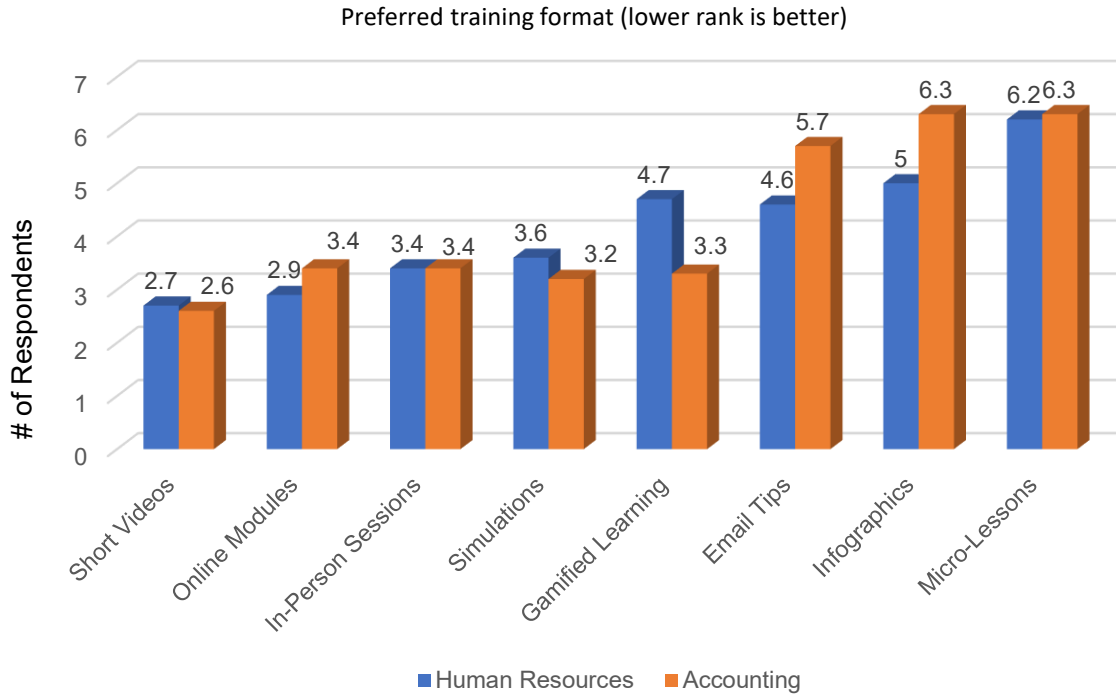
FINDINGS RQ2

Respondents perceive current campaigns as acknowledging threats but failing to teach actionable behavior.

Training fatigue evident across both departments due to repeated, non-tailored materials.



FINDINGS RQ3



Strong preference for concise, engaging, and job-relevant training.

Both departments favored video-based, scenario-driven, and interactive modules over static policy slides or email tips.

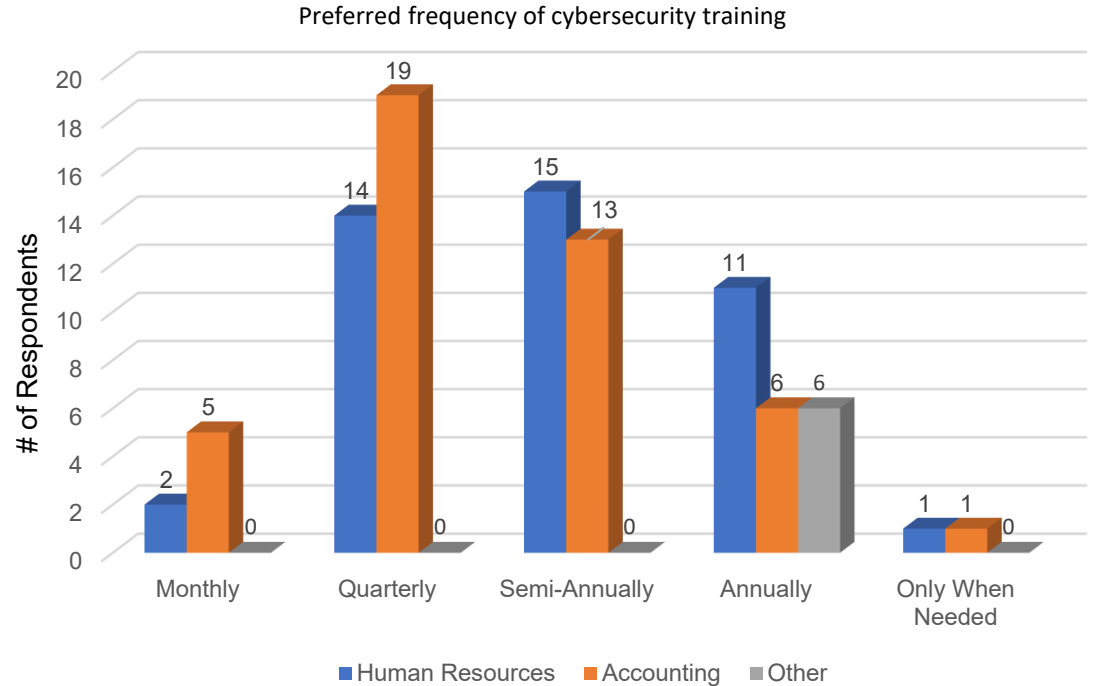
Accounting staff valued simulation-based exercises reflecting phishing and fraud scenarios.



FINDINGS RQ3

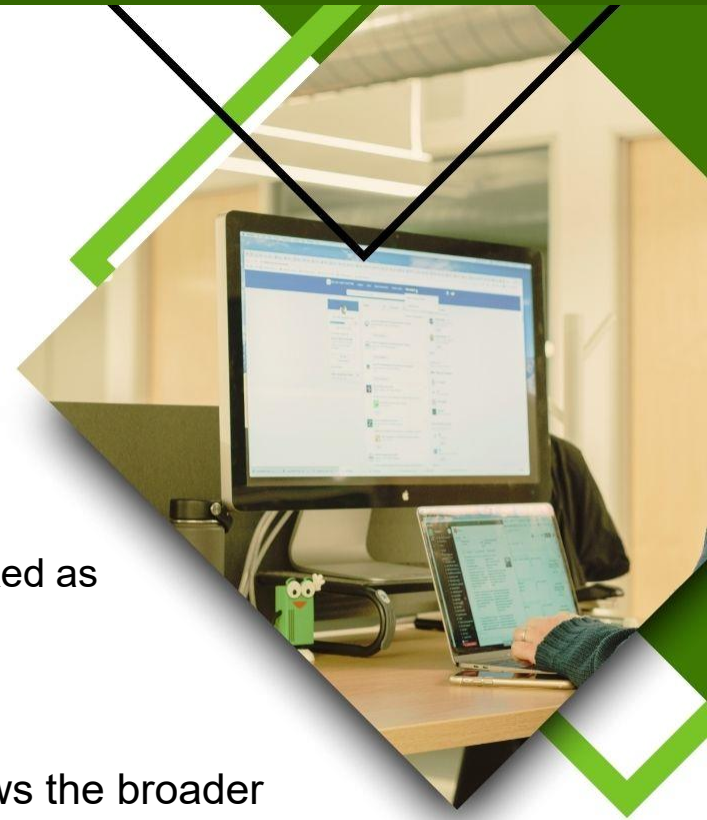
HR staff preferred self-paced and flexible learning due to diverse roles.

Adaptive learning widely supported -participants wanted to skip familiar content and focus on new or evolving topics.



VERIFICATION USING LINKEDIN SURVEYS

- ◆ Conducted public LinkedIn surveys to cross-check results from company studies.
- ◆ Survey questions replicated selected quantitative items from the HR / Accounting study.
- ◆ Findings matched closely with in-company results:
 - Phishing, data privacy, and invoice fraud again ranked as top threats.
 - Employees emphasized the need for shorter, more frequent, and role-relevant campaigns.
- ◆ Confirms external validity of earlier results and shows the broader applicability of department-specific tailoring.





LIMITATIONS

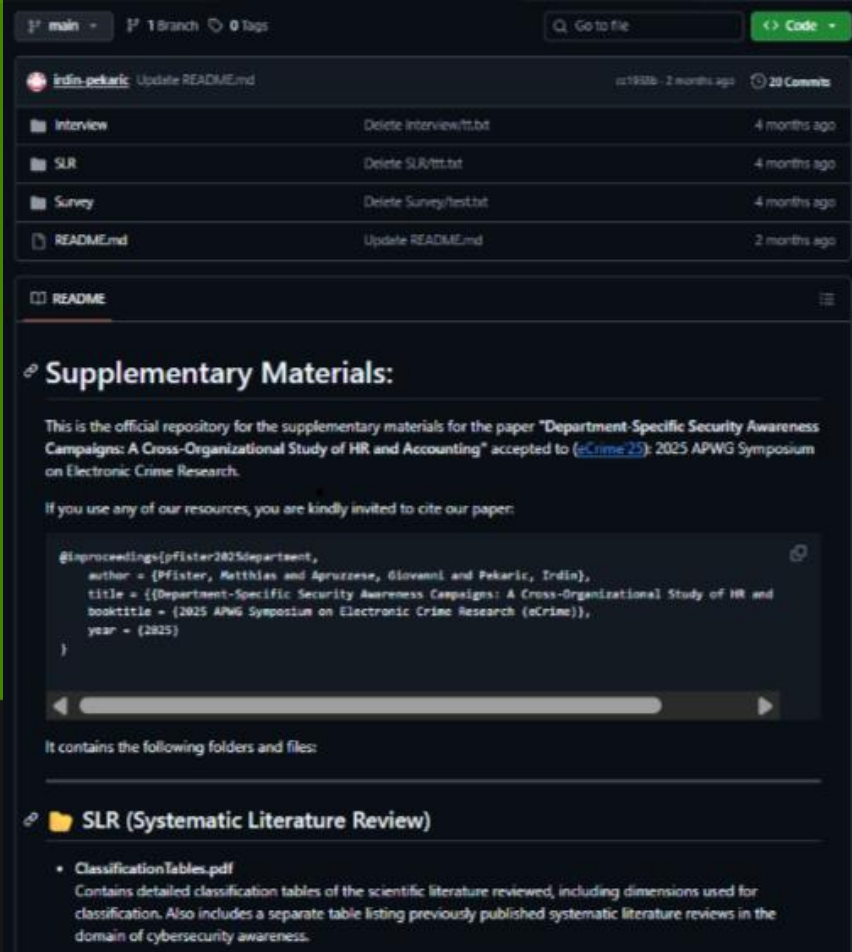
- ◆ Sample scope: Study focused only on HR and Accounting; results cannot be generalized to all departments.
- ◆ Geographical bias: Participants mainly from one region, potentially reflecting cultural and organizational specifics.
- ◆ Self-reporting bias: Interviews and surveys may reflect perceived, not actual, behavior.
- ◆ Survey distribution: Online format could introduce volunteer bias, favoring security-aware respondents.



RECOMMENDATIONS

- ❖ Tailor awareness campaigns to departmental contexts — “one-size-fits-all” is no longer effective.
- ❖ Integrate contextual scenarios reflecting daily operations (e.g., hiring, invoicing).
- ❖ Update materials regularly to avoid redundancy and maintain engagement.
- ❖ Employ adaptive learning to match employee expertise levels.
- ❖ Combine qualitative feedback with behavioral telemetry for stronger validation.





main 1 Branch 0 Tags Go to file Code

irdin-pekaric Update README.rnd 12/19/2025 - 2 months ago 20 Commits

File	Commit Message	Time
Interview	Delete Interview/ttt.txt	4 months ago
SLR	Delete SLR/ttt.txt	4 months ago
Survey	Delete Survey/ttt.txt	4 months ago
README.rnd	Update README.rnd	2 months ago

README

Supplementary Materials:

This is the official repository for the supplementary materials for the paper "Department-Specific Security Awareness Campaigns: A Cross-Organizational Study of HR and Accounting" accepted to (eCrime25): 2025 APWG Symposium on Electronic Crime Research.

If you use any of our resources, you are kindly invited to cite our paper:

```
@inproceedings{pfister2025department,
  author = {Pfister, Matthias and Apruzzese, Giovanni and Pekaric, Irdin},
  title = {{Department-Specific Security Awareness Campaigns: A Cross-Organizational Study of HR and Accounting}},
  booktitle = {(2025 APWG Symposium on Electronic Crime Research (eCrime))},
  year = {2025}
}
```

It contains the following folders and files:

- SLR (Systematic Literature Review)
- ClassificationTables.pdf

Contains detailed classification tables of the scientific literature reviewed, including dimensions used for classification. Also includes a separate table listing previously published systematic literature reviews in the domain of cybersecurity awareness.

REPOSITORY

<https://github.com/irdin-pekaric/eCrime2025>





THANK YOU

FOR YOUR ATTENTION

