

Emotions and appraisals influence whether users **click** a link in a **phishing** email.

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

Raphael Weidhaas¹, Alexandra von Preuschen², Verena Distler¹

Conditionally accepted at USENIX Symposium on Usable Privacy and Security (SOUPS) 2026

Motivation

- Technical interventions are not enough to tackle phishing
- Unclear **why** users click on phishing links
- Need to investigate psychological processes **during** phishing

Method

- Scenario study (N=41), including simulated phishing attack
- Observation, interviews, questionnaires

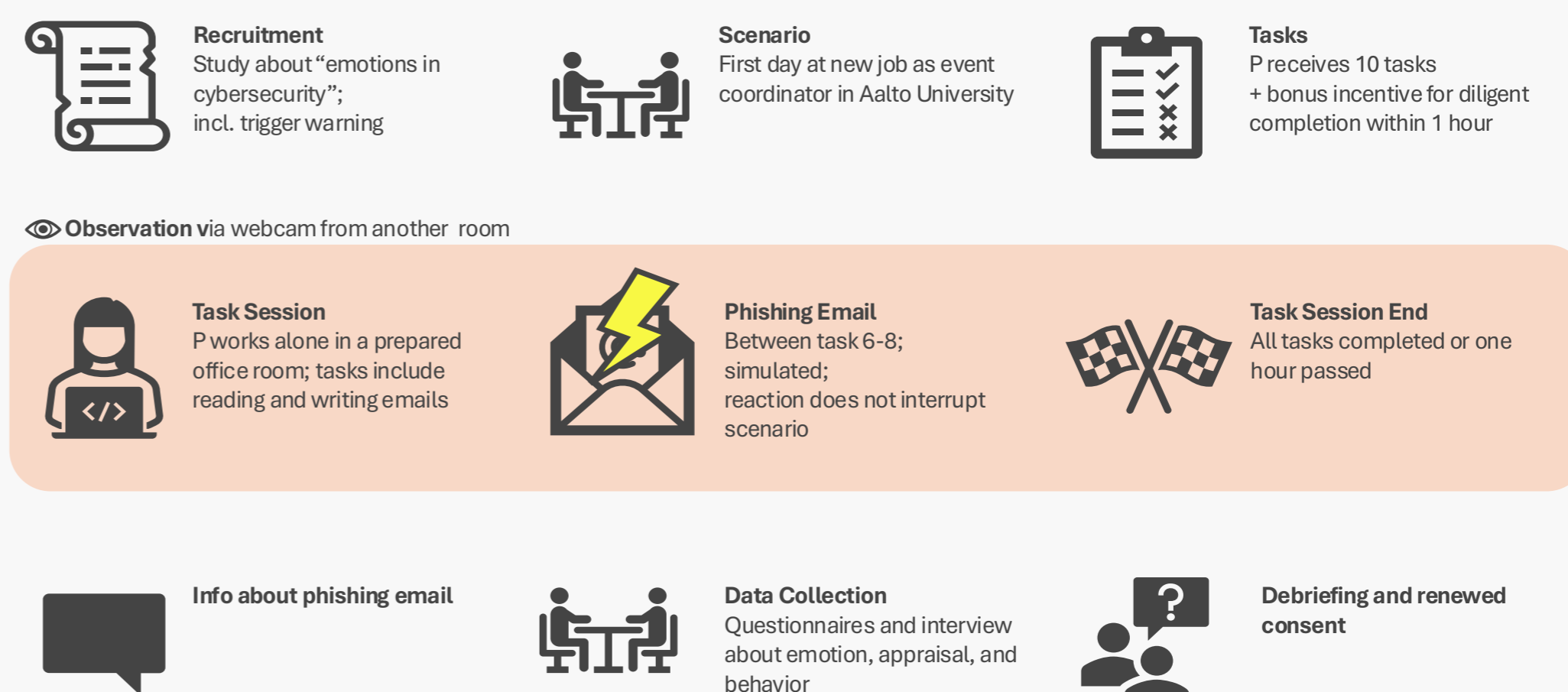
Key Takeaways

- Negative emotions led participants to stop and detect
- Phished participants appraised the phish as a problem to be solved and felt positive emotions upon providing data
- Detection produced positive emotions and self-efficacy
- Many reflected detecting the phish intuitively

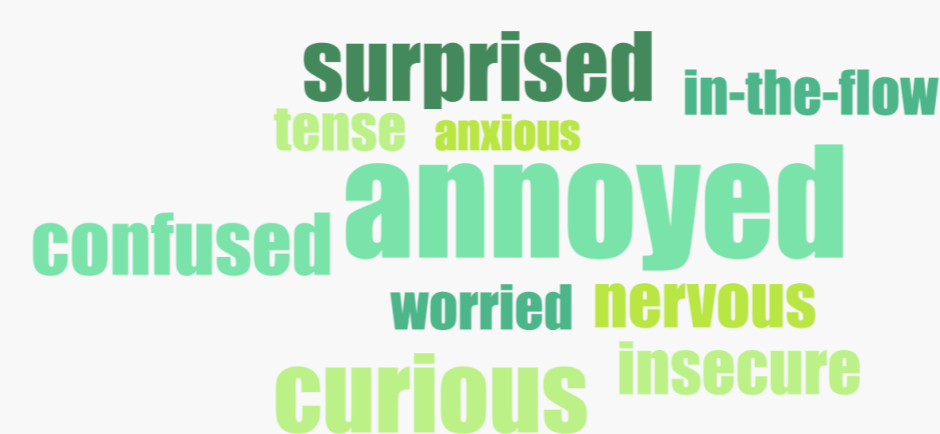
Contributions

- Bringing psychological theories of emotion to cybersecurity
- Actionable examples to improve phishing interventions
- Better understanding of secure behavior (detection)
- Novel method for realistic social engineering studies

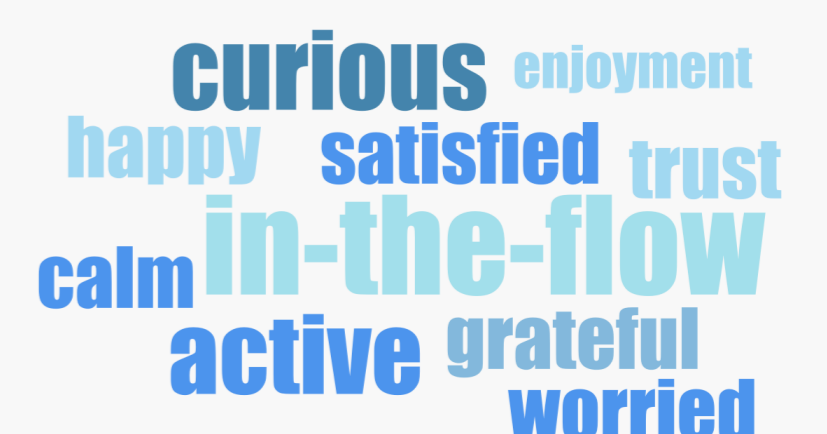
Our novel method to study social engineering in a realistic in-situ environment



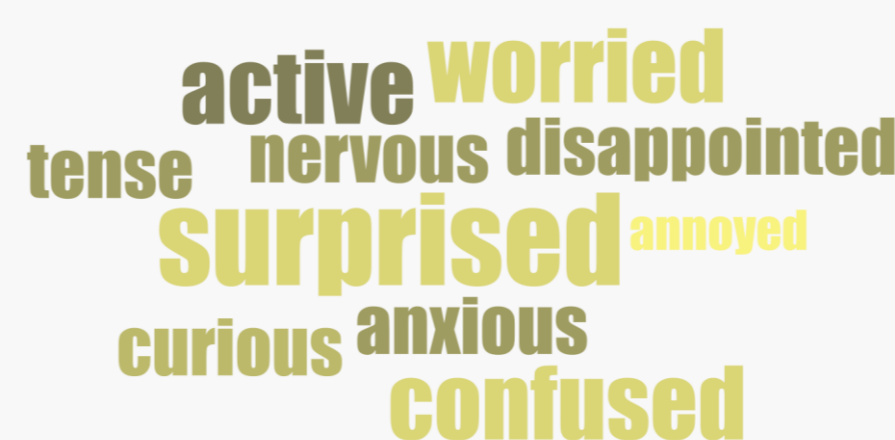
Emotions experienced during phishing



Detectors (22): Detected the phishing email



Non-detectors (7): Did not click on the phishing link, but did not detect the phishing email

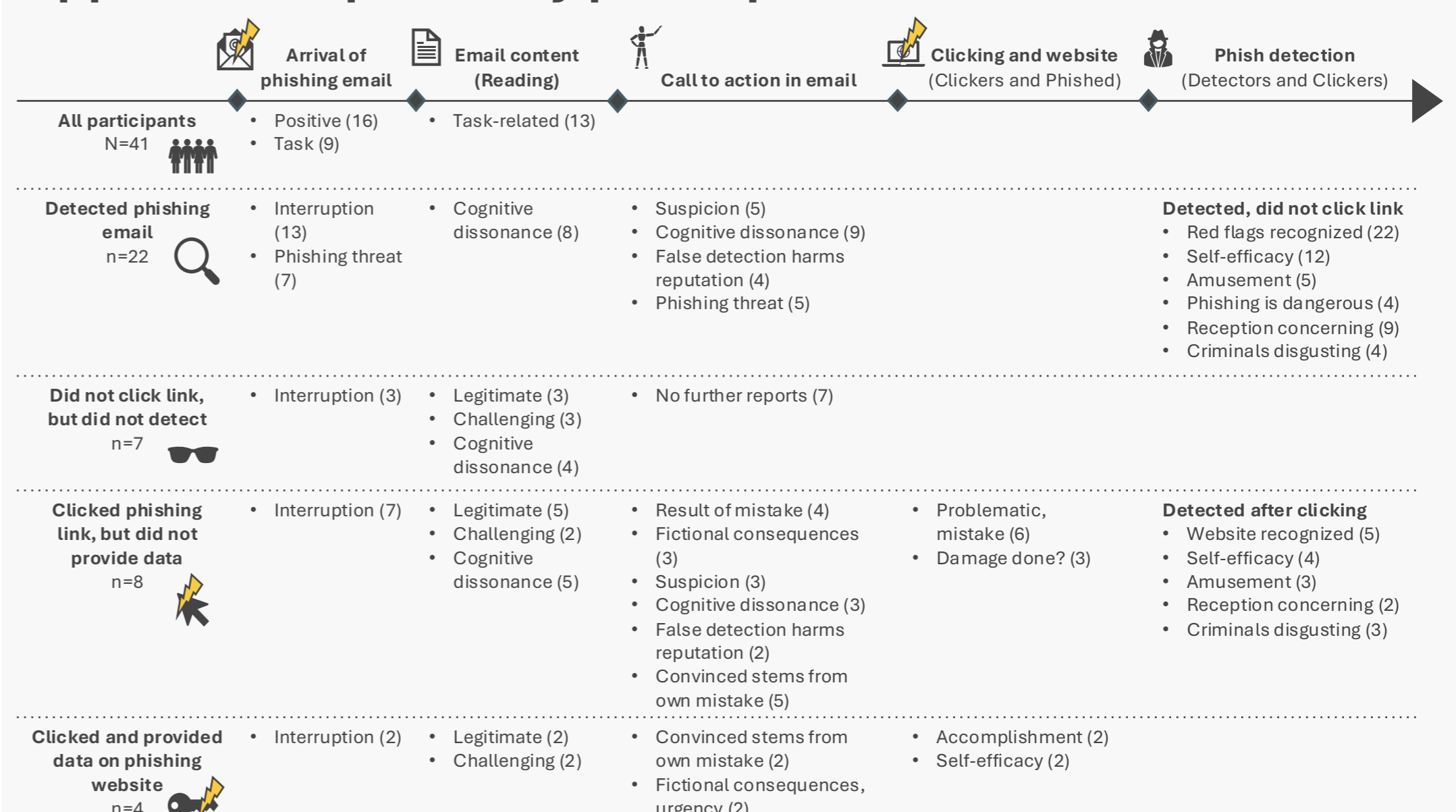


Clickers (8): Clicked on phishing link but did not provide data on phishing website



Phished (4): Clicked on phishing link and provided data on phishing website

Appraisals reported by participants



¹Aalto University, Department of Computer Science, Finland

²CISPA Helmholtz Center for Information Security, Germany