Gennaro Esposito Mocerino

Investigating Implicit Cognition in Phishing Susceptibility through the Implicit Association Test (IAT)

Tutor: Prof. Alessio Botta

Cycle: XXXIX

Year: Second

My background

- MSc degree: MSc degree in Computer Engineering from University of Naples Federico II
- DIETI Research group: Comics/ARCLab
- PhD start date: 01/11/2023
- Scholarship type: no scholarship, Computer Science Teacher in high school

Summary of study activities

- Ad hoc PhD courses / schools
  - How to boost you PhD.
  - Innovation and Entrepreneurship.
  - Scientific programming and visualization with Python.
  - 2025 Spring School on Transferable Skills

- 17 Seminars

- Conferences
  - No conferences attended

Research field of interest

- Understanding the Human Factor in Cybersecurity
  - Investigating phishing from a human-centered perspective, exploring the psychological roots of user vulnerability.
  - Bridging cybersecurity and cognitive psychology to understand both **deliberate** and **automatic** processes in phishing detection.
  - Designing human-aware defense strategies that merge technological solutions and psychological understanding.

Research activity

- Problem Statement
  - **Imagine:** you're a PhD student in computer science working on multiple projects. Between meetings, reviews, and reports, an email arrives from your coordinator: *"Please check the updated deliverable — deadline today."* The tone is formal, the layout consistent, the link seems legitimate.

  - **Question:** Would you verify the sender's address or the URL structure? Probably yes. But in the rush to meet submissions, last-minute experiments, and a coffee break you've been postponing all day — would you still notice the one character that turns a trusted domain into a trap?

Research activity

- Background
  - —Phishing isn’t just annoying — it’s costly. Organizations worldwide lose billions annually due to compromised accounts, data breaches, and productivity losses.
  - —Individuals are at risk too: even tech-savvy users can fall for attacks under time pressure or cognitive load.

- The gap in current approaches
  - —Traditional defenses rely on **slow, deliberate thinking**, such as training and explicit awareness (e.g., Spamley [1]).
  - —These strategies target the *“thinking slow”* part of the brain [2], but most phishing exploits **fast, automatic responses**.

[1] L. Gallo, D. Gentile, S. Ruggiero, A. Botta, and G. Ventre, “The human factor in phishing: Collecting and analyzing user behavior when reading emails,” Computers & Security, vol. 139, p. 103671, 2024.

[2] KAHNEMAN, Daniel. *Thinking, fast and slow*. macmillan, 2011.

The Implicit Association Test (IAT)

Congruent block

Incongruent block

Why Use IAT for Phishing?

- Why It Matters
  - — Phishing exploits **fast, automatic decisions** that bypass conscious reasoning.
  - — Social cues based on Cialdini's persuasion principles—such as urgency, authority, and familiarity—trigger implicit responses [3].
- How IAT Helps
  - — Reveals implicit biases → measures "unconscious" associations, e.g., urgent emails → immediate action, known brands → trusted.
  - — Assesses susceptibility → quantifies how users associate phishing cues with "reliable" or "unsafe."
  - — Evaluates training impact → pre/post awareness campaigns to see if implicit associations shift.
  - — Predicts real-world behavior → identifies hidden vulnerabilities even in experienced or previously victimized users.

IAT can reveals hidden, automatic phishing vulnerabilities, enabling human-centric defenses and more effective training

[3] CIALDINI, Robert B.; CIALDINI, Robert B. Influence: The psychology of persuasion. New York: Collins, 2007.

UniNa IAT: Methodology

- Design and Implementation
  - A web application designed to conduct the Implicit Association Test for understanding the role of automatic decision-making process in phishing detection or deception

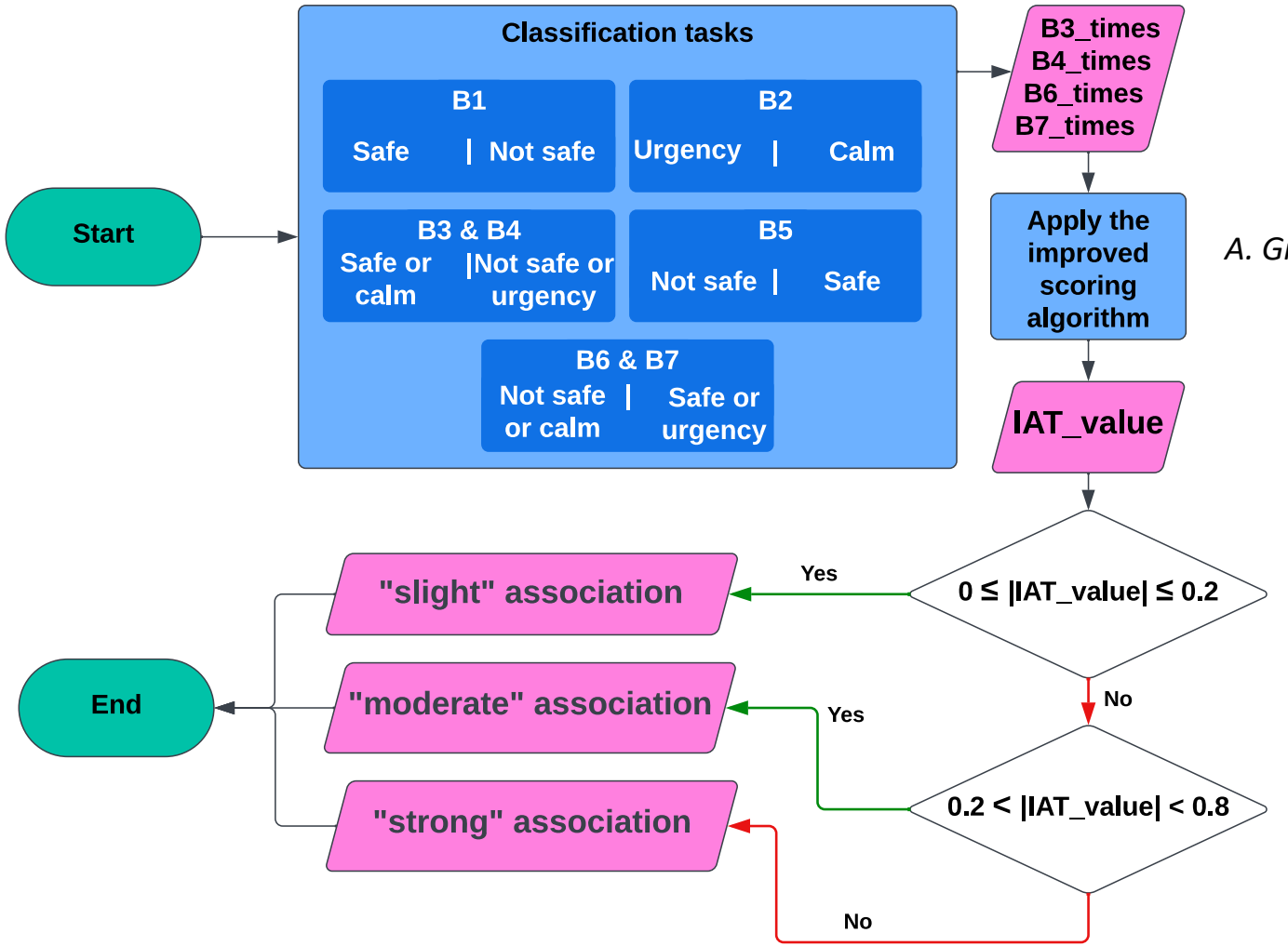
Initial Survey

IAT Test

Final Score and feedback

https://iat.comics.unina.it

UniNa IAT: Methodology



A. Greenwald et al. [3]

The Implicit Association Test (IAT) measures and standardizes classification times.

[4] Anthony Greenwald, Brian Nosek, and Mahzarin Banaji. Understanding and using the implicit association test: I. an improved scoring algorithm. Journal of Personality and Social Psychology, 85:197–216, 08 2003.

UniNa IAT: Preliminary results

- Predictive power of IAT:
  - IAT metrics show mixed correlation with past phishing victimization.
  - Self-reports may not fully reflect implicit susceptibility → explicit awareness ≠ automatic resistance.
- Implicit associations among users:
  - On average, participants **automatically sensed that phishing emails were suspicious**.
  - Responses **varied a lot between people**, depending on background, education, and experience.
  - **Beginners:** Lack implicit associations, particularly with urgency, indicating a potential cognitive vulnerability.
- Moderating factors:
  - Education & occupation strongly influence implicit susceptibility.
  - Higher education & management roles → fewer errors.
  - Certain industries & lower education → higher implicit risk.

Research products

[C1]	Gennaro Esposito Mocerino, Claudio Velotti, Danilo Gentile, Luigi Gallo, Alessio Botta, Giorgio Ventre, "Unmasking Implicit Cognitive Biases in Phishing Recognition" in 24*th* International Conference on Applied Cryptography and Network Security (ACNS), New York City, USA, 2026 – **submitted**

[C2]	Wafik P., Botta A., Gallo L., Mocerino G., Herbert C., Annicchiarico I., El Bolock A. and Abdennadher S. (2025). Enhanced Predictive Clustering of User Profiles: A Model for Classifying Individuals Based on Email Interaction and Behavioral Patterns. In Proceedings of the 11th International Conference on Information Systems Security and Privacy - Volume 2: ICISSP; ISBN 978-989-758-735-1, SciTePress, pages 363-374. DOI: 10.5220/0013302800003899 - **published**

Next year

- **Data Collection & Analysis:** Complete large-scale data collection and conduct comprehensive analyses to validate and refine the experimental framework.
- **Publication:** Consolidate findings into scientific publications, targeting at least one journal submission.
- **Dissertation:** Prepare and defend the PhD thesis, integrating all outcomes into a unified body of work.
- **Future Work:** Begin exploring advanced modeling techniques, such as preliminary machine learning analysis.

Thank you for the attention!