An Integrative Model of Phishing Susceptibility

Yuxiao “Rain” Luo – Loyola University Chicago

Adel Yazdanmehr, Nanda Kumar – Baruch College (CUNY)

Motivation and Background

- Phishing remains a dominant cyber threat (68% of data breaches).
- Despite automated defenses, human error remains a critical vulnerability.
- Fragmented behavioral research lacks a cohesive model to guide solutions.

Baruch COLLEGE | ZICKLIN SCHOOL OF BUSINESS

LOYOLA UNIVERSITY CHICAGO 1870 AD · MAJOREM · DEI · GLORIAM

In this study, we …

- Synthesize 70+ behavioral studies on phishing susceptibility.
- Identify and organize **47 constructs** across six categories.
- Propose a taxonomy and integrative model.
- Lay groundwork for future empirical testing and solution design.

Theoretical Foundations

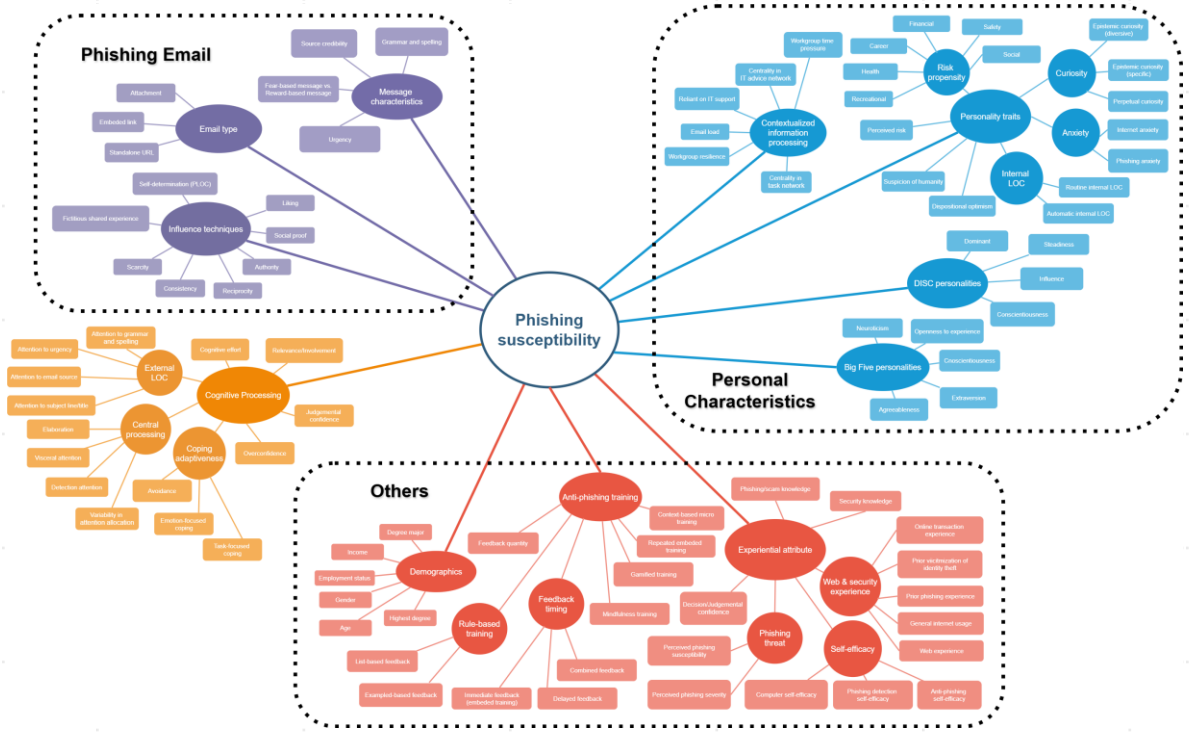
- Deception Theories (**TD, IDT**) – focus on reasoning and suspicion (Johnson et al. 1992; Buller & Burgoon 1996; Wang et al. 2017).
- Fear Appeal Models (**PMT, EPPM, FAM**) – link threat perception to coping (Maddux & Rogers 1983; Witte & Allen 2000; Johnston & Warkentin 2010).
- **TTAT** – avoidance behavior via threat and coping appraisal (Liang and Xue 2009).
- Behavioral Decision-making – **dual-process theory**, heuristics, **ELM** (Wang et al. 2012; Harrison et al. 2016).

Six Key Attributes

- **Cognitive Processing** (15 constructs) e.g., attention to urgency, cognitive effort, avoidance
- **Contextual Factors** (5 constructs) e.g., email load, group time pressure
- **Personal Traits** (11 constructs) e. g., curiosity, locus of control, DISC traits
- **Experiential Attributes** (7 constructs) e.g., phishing knowledge, efficacy
- **Influence Techniques** (5 constructs) e.g., reciprocity, scarcity
- **Message Characteristics** (4 constructs) e.g., urgency, source credibility

Integrative Model Overview

- Presents a holistic framework for understanding user vulnerability.
- Constructs are grounded in theory and literature.
- Taxonomy categorizes factors as **trait/state/contextual/experiential/influential/message**



Future Work

- Refine constructs by removing redundancy.
- Prioritize empirical variables with practical utility.
- Test model via field experiments in organizational settings.

Contributions

- **Theoretical**: Unifies fragmented behavioral findings, proposes a new taxonomy
- **Practical**: Guides design of adaptive, user-centered anti-phishing interventions.
- Addresses **AI-driven threats** where old indicators (e.g., bad grammar) are outdated.