

SECURWARE 2025

PROF. DR. ALEXANDER LAWALL

Quantifying Persuasion –

A Comparative Analysis of Cialdini's Principles in Phishing Attacks

Barcelona, 2025

RECIPROCITY



COMMITMENT



SOCIAL PROOF



AUTHORITY



LIKING



SCARCITY



Academic Roles

- Program Director, B.Sc. & M.Sc. Cyber Security and Cyber Security Management
- Professor in Cyber Security (Distance & On-site Learning)

Expertise

- System & Network Security
- Web Application & Cloud Security
- IoT and Industrial IT Security

Professional Affiliations

- Leadership Committee, "Management of Information Security" (Society for Informatics, GI)
- Professional Lead, "Security & GRC in IT" (Summit Leipzig)
- Member, Association of Cyber Forensics and Threat Investigators (ACFTI)
- Member, Zentrum Digitalisierung Bayern (ZD.B)
- Conference Committees Board Chair (IARIA)
- Steering Committee of the Conference SECURWARE & IoT-AI (IARIA)

Research & Publications

- Focus Areas: Cyber Security, Information Security, Industry 4.0/5.0, IoT, Rights Management, AI in Cyber Security
- Publications in national/international Journals and Conferences
- Keynote Speaker, Program Chair, Panel Expert of International Conferences



AGENDA

Motivation and Theoretical Foundation

1

Research Design

2

Results and Discussion

3

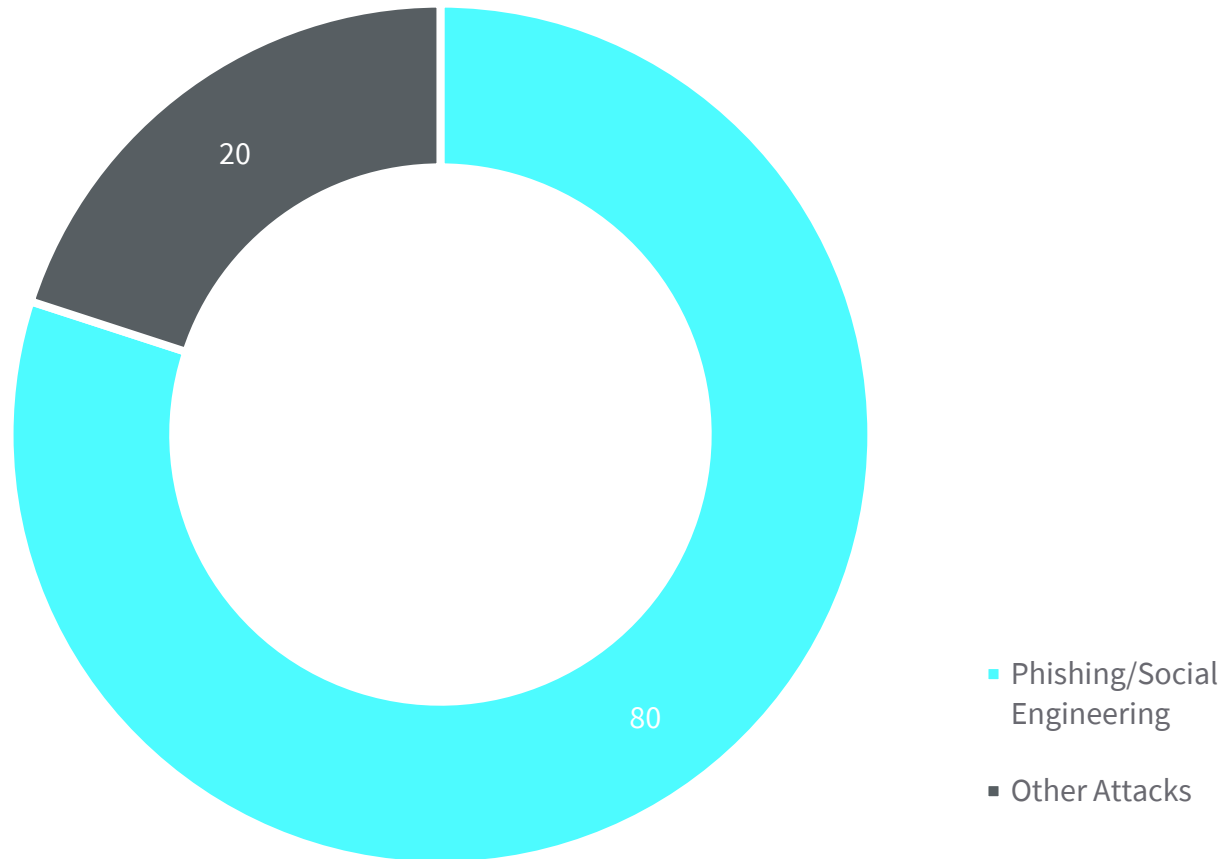
Implications for Cybersecurity

4

Conclusion and Future Work

5

Motivation



Source: "Top 70 Phishing Statistics and Trends You Must Know in 2025", 2024, [retrieved: July, 2025]. [Online]. Available: <https://keepnetlabs.com/blog/top-phishing-statisticsand-trends-you-must-know>

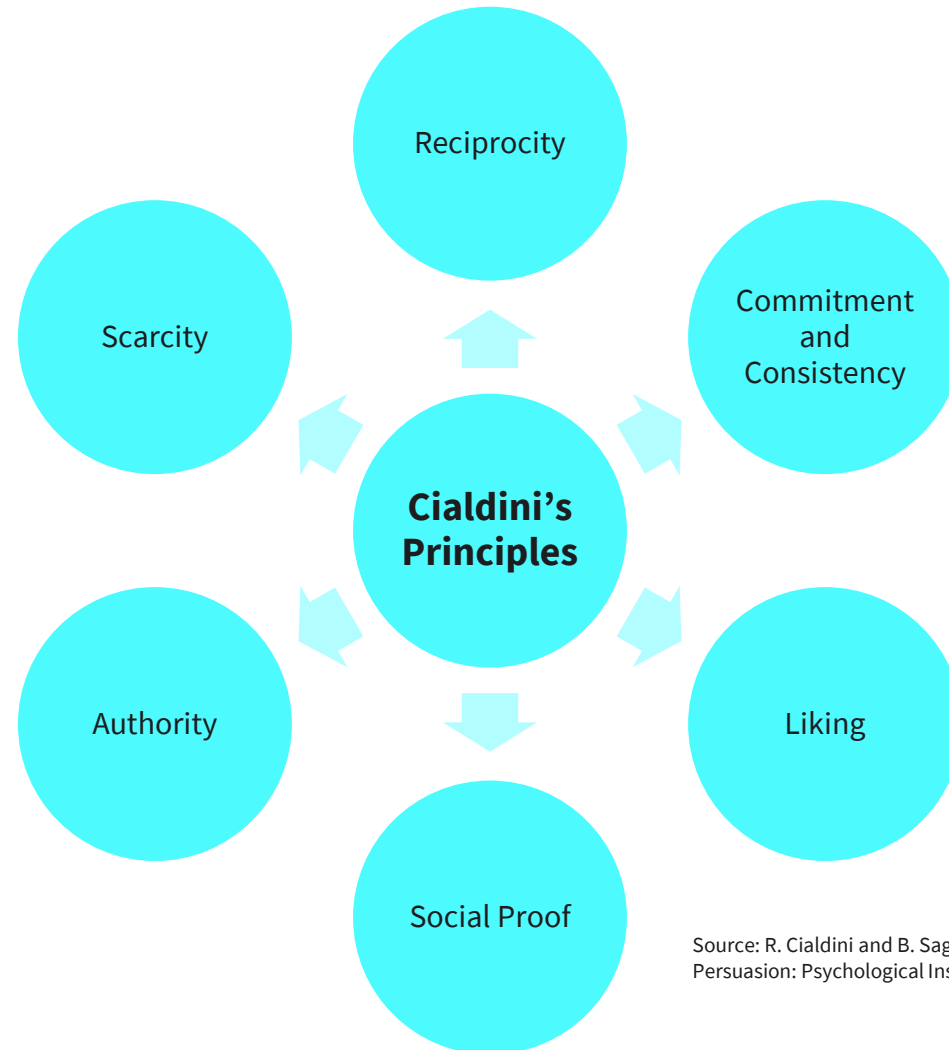
Phishing remains the leading cyber threat

What is the reason for such success based on phishing?

Which (psychological) principles drive phishing success?

MOTIVATION AND THEORETICAL FOUNDATION

Cialdini's Principles of Influence



Source: R. Cialdini and B. Sagarin, "Principles of interpersonal influence", Persuasion: Psychological Insights and Perspectives, pp. 143–169, 01 2005.

MOTIVATION AND THEORETICAL FOUNDATION

Social Engineering and Phishing Taxonomy – Attack Types



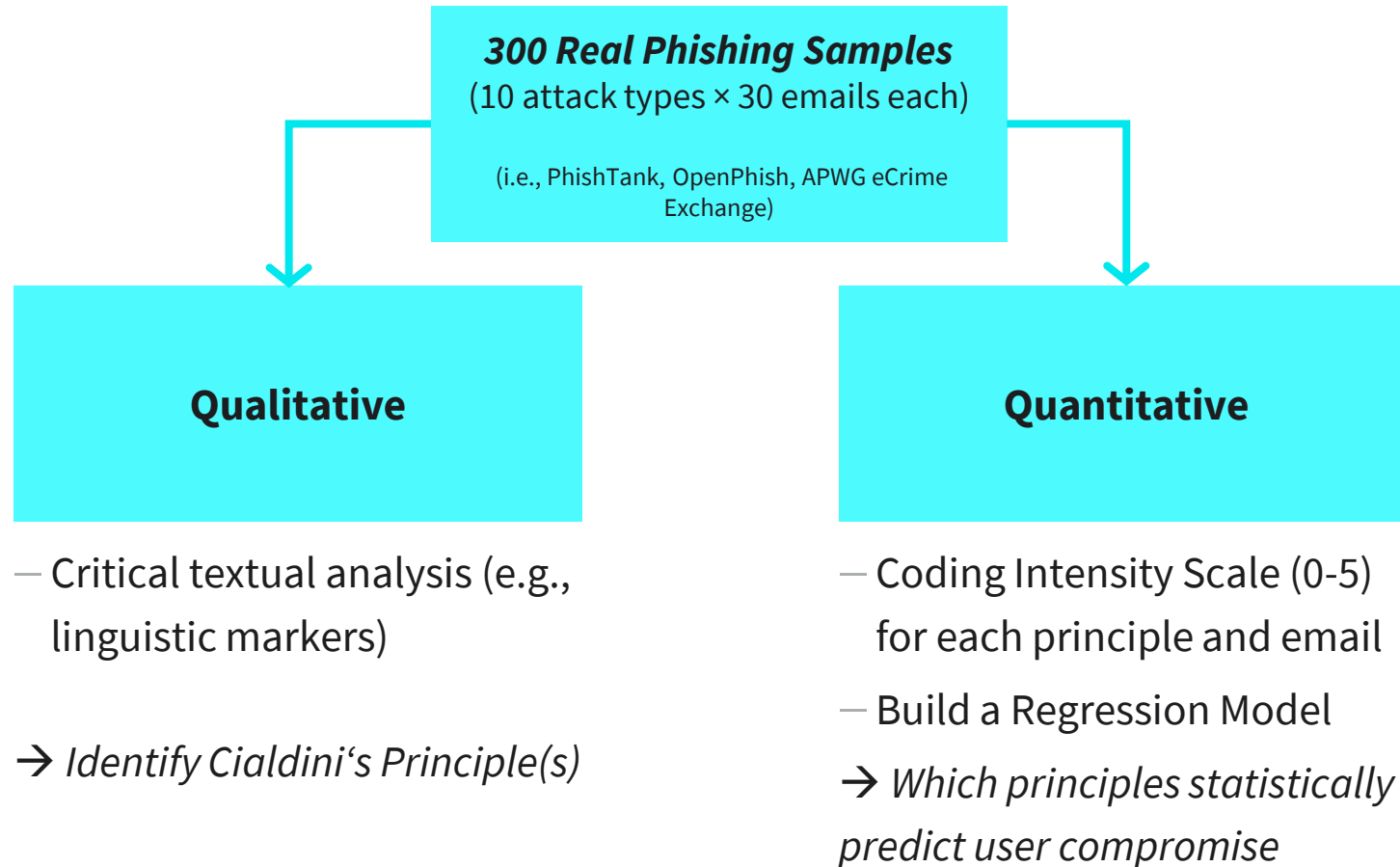
Research Questions

RQ1: How are **Cialdini's principles** of influence **exploited in real-world** phishing and spear-phishing attacks?

RQ2: What is the **statistical prevalence** of each principle across phishing types?

RQ3: Which **principles** are most strongly associated with **victim compromise**, and why?

Research Methodology: Mixed-methods Approach

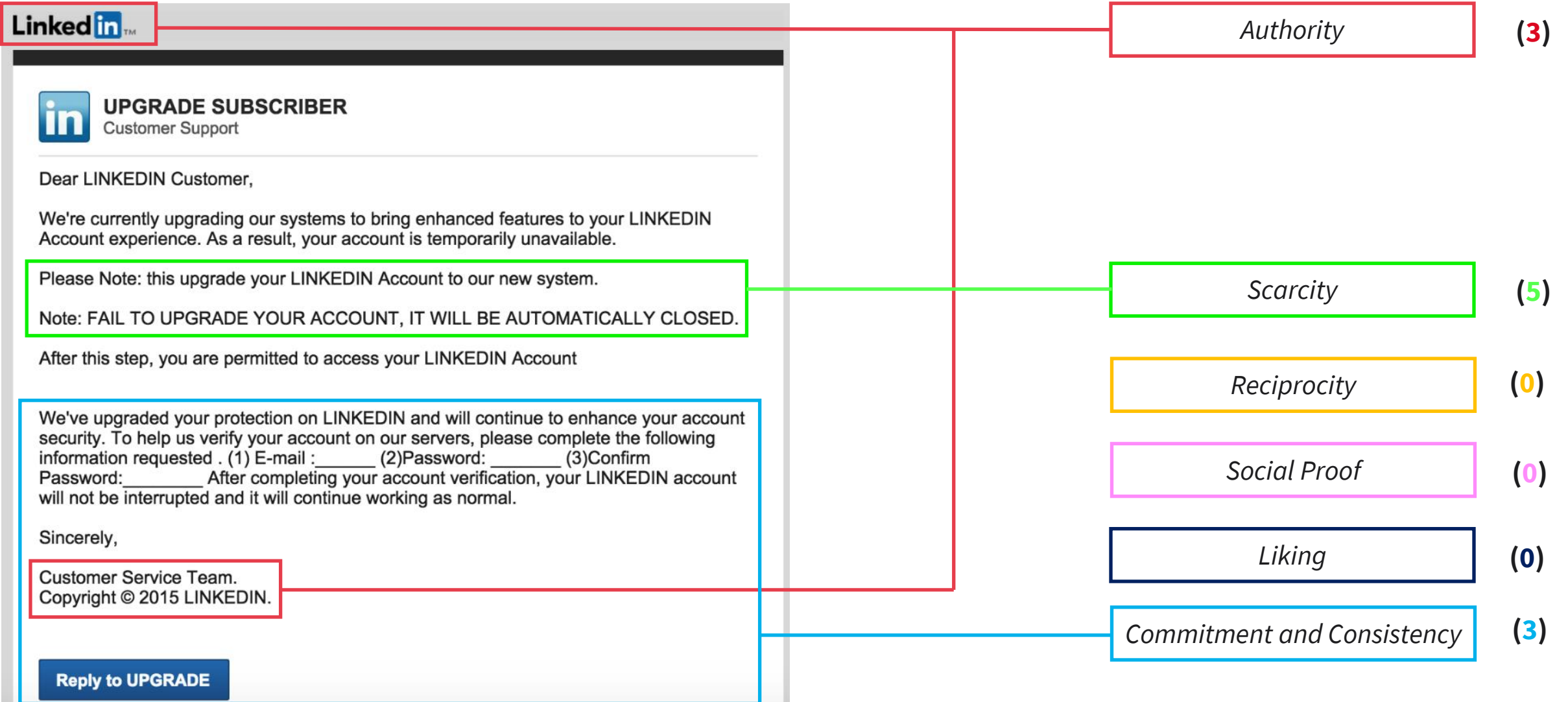


How persuasion is used, and how effective each principle is

RESEARCH DESIGN

Example

Intensity Score



RESULTS AND DISCUSSION

Relevance of Cialdini's Principles by Attack Type - Intensity Scores (Median)

Attack Type	<i>Reciprocity</i>	<i>Commit./Consist.</i>	<i>Social Proof</i>	<i>Liking</i>	<i>Authority</i>	<i>Scarcity</i>
Generic Phishing	0.00	3.00	0.00	0.00	2.00	5.00
Spear-Phishing	0.00	3.00	0.00	0.00	3.50	5.00
BEC	0.00	4.50	0.00	1.00	4.00	5.00
CEO-Fraud	0.00	5.00	0.00	1.00	5.00	5.00
Whaling	0.00	5.00	0.00	1.00	5.00	5.00
Vishing	0.00	4.50	0.00	1.00	4.00	5.00
Clone-/Dyn.-Phish.	0.00	3.00	0.00	0.00	2.00	5.00
Quishing	0.00	2.50	0.00	0.00	2.00	4.00
Smishing	0.00	2.00	0.00	0.00	2.00	5.00
AI-based Phishing	0.00	3.00	0.00	1.00	4.00	5.00

RESULTS AND DISCUSSION

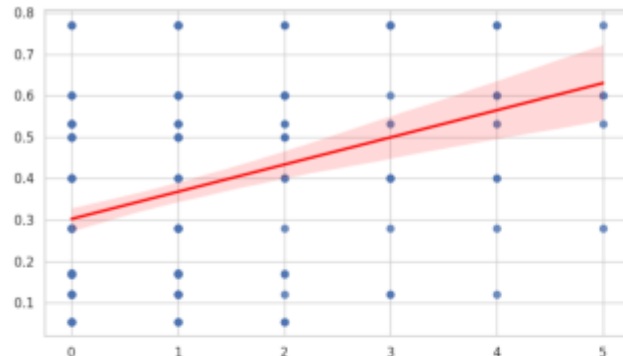
Summary of Influence Principle Prevalence and Statistical Effect

Cialdini's Principle	Median Intensity	Prevalence (%)	Regression Coefficient β	p-value
<i>Reciprocity</i>	0	11.3%	−0.0263	0.0234*
<i>Liking</i>	1	34.0%	0.6030	<0.001**
<i>Social Proof</i>	0	9.7%	0.0091	0.210
<i>Authority</i>	4	63.7%	0.2011	0.018*
<i>Scarcity</i>	5	72.1%	0.0118	0.081
<i>Commitment/Consistency</i>	3	58.0%	0.0142	0.092

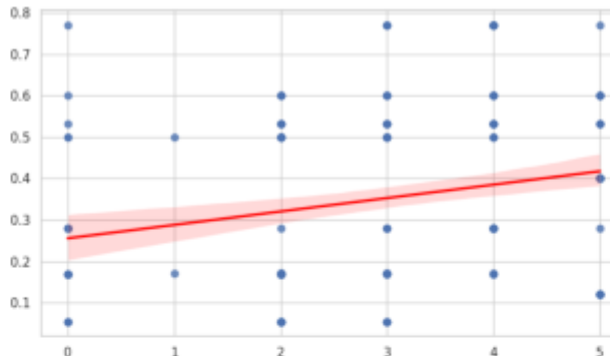
*Statistically significant at $p < 0.05$; **Highly significant at $p < 0.001$; N = 300

RESULTS AND DISCUSSION

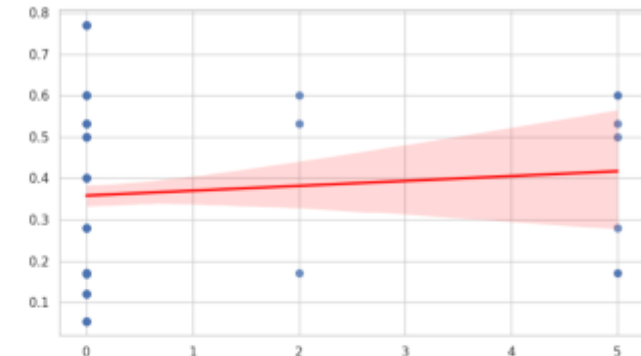
Linear Regression Plots of Cialdini Principle Intensity (x-axis) vs. Compromise Rate (y-axis)



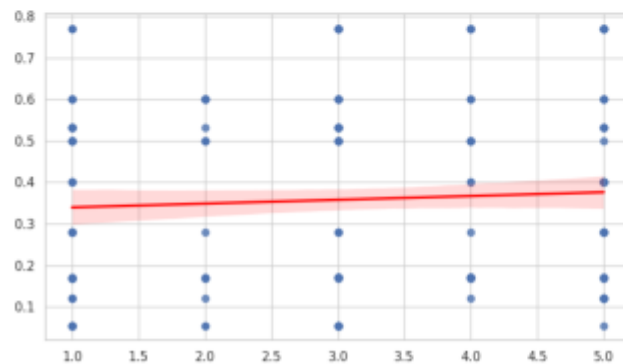
(a) Liking



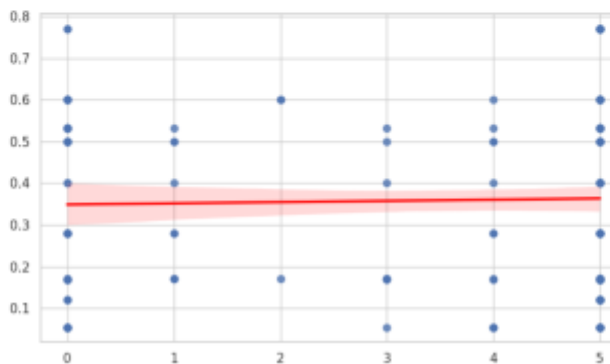
(b) Authority



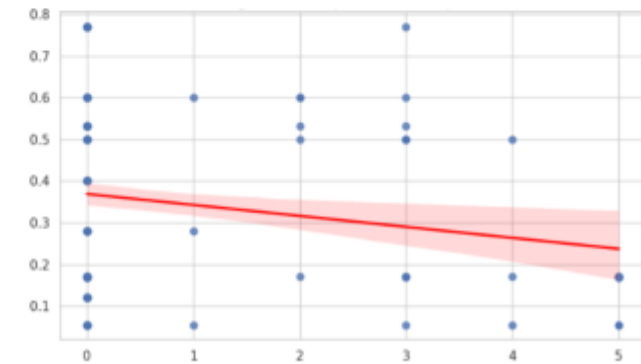
(c) Social Proof



(d) Commitment and Consistency



(e) Scarcity



(f) Reciprocity

Awareness Training:

Move from technical cues → teach psychological tactics (e.g., role-play scenarios using liking and authority cues)

Technical Defenses:

NLP-based detection of linguistic markers (e.g., urgency, hierarchical tone, affective language)

Design Recommendations:

- Context-sensitive warnings (“This message may simulate authority”)
- Cognitive interrupts for unusual requests (e.g., financial approvals)
- Highlight rhetorical structures in email clients

CONCLUSION AND FUTURE WORK

The Persuasion Paradox in Phishing: Most Used $\neq$ Most Effective

Most Used: *Scarcity*

Scarcity

- Used in ~72% of phishing emails
- Not a significant predictor of compromise

Most Effective: *Liking & Authority*

Liking

- Strongest predictor ($\beta = 0.603$, $p < 0.001$)

Authority

- significant predictor ($\beta = 0.201$, $p = 0.018$)

➤ **Attackers overuse urgency – but trust and hierarchy break defenses.**

Future Work:

- Controlled phishing simulations
- Multimodal attack vectors (text, voice, QR)
- LLM-generated phishing requiring new detection strategies
- Cross-cultural studies of persuasion in cyber contexts

If scarcity is overused but ineffective, why do attackers keep relying on it, and what does that reveal about their strategy versus our defenses?

How can we integrate psychological insights like liking and authority into technical defenses without overwhelming users with false alarms?