Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:12(3), December, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

DIGITALIZATION AND PHISHING: A SOCIO-PSYCHOLOGICAL REVIEW

[1]Ms. Gopikashree S and [2]Smt. Deepa S V

[1]Final BA (Psychology & Sociology)Government First Grade College, Yelahanka, Bengaluru ,Bengaluru City University
[2]Associate Professor, Department of Sociology,Government First Grade College, Yelahanka, Bengaluru,Bengaluru City University

Abstract

Phishing has evolved into one of the most prevalent and damaging cybercrimes in the digital era. As digitalization expands across personal, institutional, and economic spheres, cybercriminals leverage sophisticated psychological and sociological manipulation techniques to exploit human vulnerabilities. This article provides a comprehensive review of phishing from a psychological and sociological perspective, drawing on secondary data from government agencies, academic studies, and industry reports. The literature review integrates extracts from peer-reviewed research and authoritative sources to reveal the multi-layered nature of phishing susceptibility. A more precise methodology outlines the systematic procedures used for data selection and thematic analysis. Expanded discussions of psychological and sociological triggers demonstrate how attackers simultaneously exploit emotional, cognitive, and social cues. Consequences of phishing are presented at individual, organizational, and societal levels. The study identifies significant research gaps and proposes evidence-based suggestions for prevention. Findings underscore the need for integrated socio-psychological and technical approaches in combating the rising threat of phishing.

Key Words: Cybercrimes, Human vulnerabilities, Phishing, Psychological manipulation, Sociological triggers, Susceptibility

Introduction

Digitalization has transformed human interaction, economic transactions, governance, and social communication. Online platforms—email, social media, mobile applications, cloud services, and e-commerce—have become integral to daily life, bringing convenience but also unprecedented security vulnerabilities. Phishing, a deceptive cyberattack that manipulates individuals into revealing confidential information or performing harmful actions, has emerged as one of the most dominant cyber threats globally. Reports from law enforcement and cyber-intelligence agencies show staggering increases in phishing activity. The Anti-Phishing Working Group (APWG, 2025) notes that phishing attempts "continue to set new records quarter after quarter," with nearly one million attacks documented in late 2024 and early 2025. The FBI Internet Crime Complaint Center (IC3, 2024) labels phishing as "the single most frequently reported cybercrime," with elderly victims experiencing disproportionate financial losses. The expansion of digital systems has created fertile ground for cybercriminals to exploit psychological vulnerabilities and sociological structures. Understanding phishing from both perspectives is vital.

Review of Literature

Growth of Phishing in a Digitalizing World

Industry reports highlight correlations between digital expansion and cyber-crime escalation. APWG (2025) documents nearly 1,003,924 phishing attacks in one quarter alone. The FBI/IC3 report states: "Phishing and spoofing-related complaints outrank all other categories, cutting across all age groups, industries, and demographic backgrounds." Elderly victims faced the highest losses.

Psychological Perspectives

Scholars highlight individual cognitive and emotional processes. Frauenstein and Flowerday (2020) emphasize: "Phishing attacks exploit heuristic processing, whereby individuals under cognitive load rely on mental shortcuts rather than deliberate

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:12(3), December, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

reasoning." Ribeiro et al. (2024) state: "A user's belief in their ability to detect phishing significantly predicted resilience, whereas overconfidence without actual skill increased risk." Impulsivity, neuroticism, and low awareness correlate with susceptibility.

Sociological Foundations

Phishing exploits cultural norms, institutional trust, and social networks. Siddiqi et al. (2022) assert: "Social engineering-based attacks succeed because they mimic authoritative communication patterns ingrained within organizational life." Interpersonal trust—especially via social media or messaging apps—further increases vulnerability. Structural inequality also shapes susceptibility, with elderly users experiencing lower digital literacy and young users showing higher impulsivity.

Research Gap

While numerous empirical and industry reports document incidence and outline psychological mechanisms, gaps remain:

a. **Integrated psycho-sociological models** — Existing studies often examine individual cognitive or demographic predictors in isolation; fewer studies model interactions between personality, group norms (e.g., workplace culture), and macro-level digital ecosystems.
b. **Longitudinal victim trajectories** — Limited longitudinal evidence tracks how repeated exposure or prior victimization changes behavior over time.
c. **Contextualized interventions** — There is a shortage of intervention studies that simultaneously test technical, educational, and sociological remedies in real organizational settings.
d. **AI and emergent vectors** — Rapid developments in AI-assisted phishing require updated behavioral research to test whether classic triggers operate similarly when messages are hyper-personalized.

Addressing these gaps will improve predictive models and the design of layered mitigations.

Objectives of the Study

1. To synthesize recent empirical and industry evidence on phishing incidence and victim profiles.
2. To describe and analyze psychological mechanisms (cognitive biases, personality traits) that underpin susceptibility.
3. To explore sociological factors (trust, organizational culture, social scripts) that enable phishing success.
4. To identify triggering elements used by phishers and profile likely victim groups.
5. To provide evidence-based suggestions for prevention combining psychological, sociological, and technical strategies.

Methodology of the Study

A systematic qualitative synthesis approach is used. A mixed-method systematic review combining narrative synthesis, document analysis, and thematic coding.

Data Sources

Peer-reviewed journals, government reports (FBI/IC3), industry reports (APWG, Fortinet), and verified cyber security publications.

Reliability and Validation

Triangulation across academic, government, and industry sources ensured reliability.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:12(3), December, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

Psychological Perspectives on Phishing

a. **Cognitive Biases:** Phishing exploits authority bias, urgency bias, availability bias, and consistency bias. Dual-process theory shows that heuristic reasoning dominates under stress or distraction.
b. **Emotional Manipulation:** Attackers exploit fear ("Your account is locked"), greed (prizes), curiosity (unexpected attachments), and compassion (help requests)
c. **Personality Factors:** Impulsivity, neuroticism, and overconfidence significantly elevate risk.

Sociological Perspectives on Phishing

1. **Authority and Compliance:** Culturally rooted obedience to authority increases compliance.
2. **Social Proof:** Statements like "Your colleague has completed verification" create conformity.
3. **Institutional Trust:** Messages imitating banks or government agencies evoke automatic trust.
4. **Interpersonal Trust:** Friends' and colleagues' compromised accounts amplify susceptibility.

Socio-Psychological Triggering Elements of Phishing

Phishing blends emotional, cognitive, and social manipulation:

a. **Psychological Triggers:** Fear, anxiety, urgency, Novelty, curiosity, Greed, rewards**,** Reciprocity, and helpfulness.
b. **Sociological Triggers:** Cultural communication norms, Organizational hierarchy, Social proof, peer pressure, Informal digital channels (WhatsApp groups), High-trust environments.
c. **Technological Triggers:** AI-personalized messages, Spoofed URLs, Deep fake audio/video impersonation, and Mobile interface constraints.

Possible Victims of Phishing

High-risk groups include: Elderly users with low digital literacy, Young users with high impulsivity, Employees in stressful digital workplaces, Social media-intensive users, and Organizations lacking a cybersecurity culture

Consequences of Phishing

Socio-Psychological Triggering Elements of Phishing

Phishing attacks are carefully crafted to manipulate both individual cognitive biases and collective social norms. These triggers operate in three layers:

1. Cognitive Triggers (Psychological)

a. Authority Bias: People tend to obey messages appearing to come from banks, government, or senior officials.

b. Urgency and Scarcity: Attackers intentionally create time pressure ("Your account will be locked in 2 hours") to disable rational analysis.

c. Curiosity and Novelty: Unexpected attachments or rewards spark impulsive clicking.

d. Fear Appeals: Threats about financial loss, legal consequences, or security breaches evoke panic-driven responses.

e. Reciprocity: Requests framed as needing "urgent help" exploit social obligation norms.

These triggers align with the dual-process theory: users shift to fast, heuristic reasoning under emotional arousal.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:12(3), December, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

2. Social Triggers (Sociological)

a. Social Proof: Messages indicating others have already complied ("Your team completed verification") reduce skepticism.

b. Cultural Scripts: Attackers imitate legitimate communication patterns within specific cultures or workplaces.

c. Interpersonal Trust: Messages from compromised accounts of friends or colleagues exploit relational closeness.

d. Hierarchical Compliance: In cultures where authority is respected, impersonation of superiors significantly increases compliance.

e. Routine Digital Habits: People accustomed to multitasking may click links automatically without scrutiny.

3. Technologically Amplified Triggers

a. AI-generated personalization makes phishing more convincing through tailored language, writing style, and contextual cues.

b. Device-level factors: Mobile users make more errors due to smaller screens and link-masking.

The combination of psychological emotion-driven cues and sociological trust-driven cues makes phishing uniquely dangerous.

Consequences of Phishing

Phishing has multi-level impacts that extend beyond financial losses.

1. Individual Consequences

a. Financial Losses: Victims may lose savings, be manipulated into transfers, or experience unauthorized account activity.

b. Identity Theft: Stolen credentials can be resold, resulting in long-term harm such as credit damage.

c. Emotional Trauma: Feelings of shame, guilt, fear, and self-blame are common—especially among elderly victims.

d. Digital Trust Erosion: Victims may become reluctant to use online banking, e-commerce, or e-governance platforms.

A 2024 IC3 report notes that victims "often experience prolonged anxiety, lack of confidence, and fear of using digital systems."

2. Organizational Consequences

a. Data Breaches: Phishing is the leading initial vector in corporate intrusions.

b. Business Email Compromise (BEC): BEC attacks result in multimillion-dollar losses globally.

c. Reputational Damage: Compromised organizations face customer distrust and brand erosion.

d. Operational Disruption: Malware or ransomware delivered via phishing can halt corporate functioning.

3. Societal Consequences

a. Public Trust Decline: Widespread scams reduce faith in digital transformation initiatives.

Cover Page

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY EDUCATIONAL RESEARCH
ISSN:2277-7881(Print); IMPACT FACTOR :9.014(2025); IC VALUE:5.16; ISI VALUE:2.286
PEER REVIEWED AND REFEREED INTERNATIONAL JOURNAL
(Fulfilled Suggests Parameters of UGC by IJMER)
Volume:14, Issue:12(3), December, 2025
Scopus Review ID: A2B96D3ACF3FEA2A
Article Received: Reviewed: Accepted
Publisher: Sucharitha Publication, India
Online Copy of Article Publication Available: www.ijmer.in

b. Economic Burden: Law-enforcement costs, insurance claims, and preventive investments strain public resources.

c. Rise in Organized Cybercrime: Profits from phishing often fund larger criminal networks.

Thus, phishing has psychological, economic, social, and infrastructural implications that go far beyond the individual victim.

Suggestions

A layered, psycho-sociotechnical approach is recommended:

a. Technical controls (first line): robust email filtering, domain-verification (DMARC/DKIM/SPF), URL sandboxing, and device-level protections. Keep these updated to address AI-generated variants.
b. Behavioral training that targets cognitive biases: move beyond awareness slides to scenario-based training that simulates emotional triggers, teaches verification rituals (e.g., out-of-band confirmation for financial requests), and improves detection self-efficacy. Feedback and adaptive training reduce overconfidence.
c. Organizational policies and social norms: enforce verification norms (e.g., "no financial action without 2-factor verification"), limit information exposure on public profiles, and create clear incident reporting channels that avoid blame.
d. Sociotechnical interventions: redesign workflows to remove single-actor points of failure for high-risk transactions and adopt approval rails that require multi-party signoff for transfers.
e. Support for high-risk groups: targeted outreach for older adults and low-literacy populations, including community workshops, simplified verification tools, and faster remediation support.
f. Research & policy: fund longitudinal studies on behavior change and test combined technical/educational interventions in field settings. Broaden regulation to make impersonation harder (stronger anti-spoofing enforcement and domain takedown processes).

Conclusion

Phishing is a complex socio-psychological phenomenon requiring integrated interventions. As digitalization deepens, cybercriminals exploit cognitive biases, social structures, and emotional vulnerabilities. Literature reveals an interplay of psychological and sociological factors shaping susceptibility. Future efforts must combine technical, educational, and policy-based solutions to enhance resilience against phishing.

References

1. Anti-Phishing Working Group. (2025). Phishing activity trends report: Q1 2025. APWG.
2. Federal Bureau of Investigation. (2024). IC3 annual report. FBI.
3. Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites. Computers & Security, 94, 101862.
4. Kavvadias, A., et al. (2025). Understanding demographic and psychological factors in phishing susceptibility. Applied Sciences, 15(4), 2236.
5. Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Predictors of phishing susceptibility. Computers & Security, 136, 103558.
6. Siddiqi, M. A., et al. (2022). Psychology of social engineering. Applied Sciences, 12(12), 6042.