IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

A Study on Individual Susceptibility to Phishing Attacks via Social Engineering in Bengaluru, India

Dr. Ranjithkumar S[1] and A Priya Shekinah[2]
Professor, School of Economics and Commerce, CMR University, Bengaluru, India[1]
6th B Com IAF, School of Economics and Commerce, CMR University, Bengaluru, India[2]

Abstract: *Phishing attacks are evolving rapidly, often using psychological tricks—known as social engineering—to take advantage of human behavior. This study looks at how vulnerable individuals in Bengaluru, India, are to such attacks, focusing on their awareness, reactions, and exposure to these deceptive tactics. An online survey was conducted to gather primary data with 55 participants from diverse backgrounds.*

While most respondents had heard of phishing, many struggled to recognize red flags like urgent messages, fear-based prompts, or impersonation. The responses showed a tendency to act quickly when under emotional pressure, making these social engineering techniques highly effective. Despite growing awareness, practical safety habits—such as enabling two-factor authentication or reporting suspicious activity—were found to be underused.

Unearthing this suggests that simply being aware about phishing isn't enough. Real protection requires a better understanding of the psychological triggers at play and more focused behavioral training. This study adds to the growing conversation about the human side of cybersecurity and offers clear, practical steps to help individuals better protect themselves.

Keywords: Phishing Attacks, Social Engineering, Cybersecurity Awareness, Human Vulnerability, Behavioural Response, Individual Susceptibility, Online Deception

I. INTRODUCTION

Phishing has become one of the most common and successful forms of cybercrime in recent years. Instead of relying only on technical weaknesses, phishing attacks often exploit human psychology to deceive individuals into revealing sensitive information. This method of manipulation is widely known as social engineering. It uses psychological methods like urgency, fear, or impersonation to create a false sense of trust or panic in the target.

Phishing can affect anyone - regardless of their age, occupation, or technological knowledge. While organizations have started investing in employee training and cybersecurity tools, individual users remain highly vulnerable. In India, the rapid rise of digital platforms and online services has made individuals even more exposed to such threats. Yet, public understanding of how phishing works - especially the psychological tricks used - is still limited.

This study focuses on individuals in Bengaluru, India, and aims to understand their awareness, behavior, and susceptibility to phishing attacks via social engineering. It identifies common behavioral patterns and response tendencies among individuals when faced with suspicious or manipulative messages. This was done by collecting primary data through a structured online survey. It also evaluates how emotional triggers and lack of preventive habits contribute to the success of these attacks.

Statement of the Problem

The decision to explore the topic of phishing attacks through the lens of social engineering was driven by both personal interest and increasing concern. Over the past few years, particularly following the COVID-19 lockdown, I began to notice a sharp rise in the number of phishing incidents shared by people around me—friends, relatives, and acquaintances. Many had either fallen victim to online scams or had narrowly escaped one. These conversations, coupled with the frequent reporting of such cases in the news, sparked a genuine curiosity in me about how these scams

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 8, May 2025 Impact Factor: 7.67

are carried out and why they continue to succeed. Having always been intrigued by the psychological techniques used in social engineering, I felt compelled to understand phishing beyond its surface-level definitions. Once I narrowed down my focus to phishing attacks, I wanted to explore not only the technical aspects but also how ordinary individuals perceive and respond to them. This inspired me to conduct a primary survey among people in my own circles to better understand awareness levels, personal experiences, and emerging behavioral patterns related to phishing. Through this research, I aimed to bridge the gap between public perception and actual preparedness in dealing with such threats.

II. REVIEW OF LITERATURE

Lack of Awareness and Reporting Behavior

Several studies highlight a gap between knowing what phishing is and being able to spot it. A multivocal literature review by Hijji and Alam (2021) found that "awareness often fails to translate into practical caution. Moreover, preventive habits such as reporting phishing emails or enabling security features like two-factor authentication remain uncommon, especially among general users".

This disconnect is echoed in the findings of the current study, where many respondents were familiar with phishing in theory but did not apply preventive behaviors in practice.

Social Engineering and Phishing Attacks

Marcus Butavicius et al. (2021) observed that "phishing and spear-phishing emails often bypass technical filters by targeting human behavior, particularly during emotionally loaded situations". This supports the growing belief that human psychology, not system weakness, is the primary vulnerability in phishing scenarios.

Phishing attacks are among the most widespread forms of cybercrime, often relying on social engineering rather than technical breaches. Social engineering is the act of manipulating people into performing actions or revealing confidential information, usually by exploiting emotions like fear, urgency, trust, or greed. According to Workman (2008), "these attacks often succeed not because of technological sophistication but due to the human tendency to trust perceived authority and familiarity".

Psychological Manipulation in Phishing

Keith Jones et al. (2020) examined vishing (voice-based phishing) and revealed that "attackers frequently use persuasion principles such as authority, scarcity, and social proof". These same principles are mirrored in online phishing attempts as well, often leading to impulsive decision-making. The manipulation of psychological vulnerabilities—rather than just exploiting ignorance—makes phishing a uniquely dangerous threat.

Individual Susceptibility and Behavioral Triggers

Ana Ferreira and Gabriele Lenzini (2020) identified that "emotional appeals and cognitive overload are common tactics that decrease users' ability to judge authenticity accurately". Nicholson, Coventry, and Briggs (2017) explored how individuals respond to phishing emails and found that "social salience cues, such as sender identity and urgency, significantly affect whether users recognize fraudulent messages".

Our study builds on these ideas by exploring how real people in a diverse urban Indian context react to phishing under different emotional triggers, offering a localized perspective on susceptibility.

Research Gap

Existing research focuses heavily on workplace phishing, corporate training, or Western contexts. However, there is limited empirical data that explores how everyday individuals—outside of a corporate environment—perceive and respond to phishing threats, especially in Indian cities like Bengaluru. This study seeks to bridge that gap by providing primary data and analysis on individual behavioral patterns, awareness levels, and emotional responses to social engineering tactics.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

Objectives of the Study

This study aims to:

- To analyze behavioral responses and susceptibility patterns toward phishing attempts.
- To recognize common psychological triggers that affect victims' choicess.

III. RESEARCH METHODOLOGY

This study uses a **quantitative empirical research design** to examine the susceptibility of individuals in Bengaluru to phishing attacks. It was an original investigation into how individuals – not companies or employees, but regular people from the researcher's own community and demographic mix – experience and respond to phishing attacks using social engineering. The participants were selected using convenience sampling, including a variety of students, working professionals, homemakers, and others from diverse age groups and backgrounds. An online questionnaire was used to collect valuable insights from them.

A total of 55 individuals responded to the questionnaire, providing a varied sample for analysis. Data collection was done through a Google Forms survey, which included multiple-choice and rating-scale questions. These questions intended to understand:

- The participants' awareness of phishing
- Their behavior when faced with suspicious messages
- Their recognition of social engineering techniques
- The security practices they follow

The survey link was shared through social media, email and personal contacts over the period of two weeks. All the participants were informed about the nature of the study and gave their consent prior to their contribution. To ensure honest answers and protect privacy, the responses were collected anonymously

IV. DATA ANALYSIS AND INTERPRETATION

Table 1 - Demographic Factors

Basis	Particulars	Frequency	Percentage
Age	Under 18	2	3.6
	18 - 25	34	61.8
	26 - 35	7	12.7
	36 - 45	7	12.7
	46 - 55	2	3.6
	56 and above	3	5.5
	Total	**55**	**100**
Gender	Male	31	56.4
	Female	24	43.6
	Total	**55**	**100**
Occupation	Student	30	54.5
	Working professional	18	32.7
	Self - employed	4	7.3
	Homemaker	2	3.6
	Retired	1	1.8
	Total	**55**	**100**
	Rarely	3	5.5
	A few times a week	1	1.8
	Daily	19	34.5

DOI: 10.48175/IJARSCT-26936

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

Internet Usage	Multiple times a day	32	58.2
	Total	**55**	**100**

The data collected through a structured online survey of 55 respondents provided valuable insight into individuals' awareness levels, behavioral patterns, and emotional responses to phishing attacks in Bengaluru, India. Demographic characteristics are summarized in **Table 1**, which outlines the – age, gender, occupation and internet usage – frequency of the sample. A majority of respondents were in the 18–25 age group and identified as students or young professionals, reflecting a digitally active demographic frequently exposed to online risks.

Table 2 - Awareness of Phishing

Basis	Particulars	Frequency	Percentage
Awareness of 'Phishing' Term	Yes	46	85.6
	No	9	16.4
	Total	**55**	**100**
Self - assessed understanding	Very good	13	23.6
	Somewhat good	18	32.7
	Limited	15	27.3
	None at all	9	16.4
	Total	**55**	**100**
Formal phishing training exposure	Yes	28	50.9
	No	27	49.1
	Total	**55**	**100**
Exposure to fraudulent requests for personal data	Yes	36	65.5
	No	13	23.6
	Not sure	6	10.9
	Total	**55**	**100**

As shown in **Table 2** most participants reported having heard of phishing, and many recognized common cues such as suspicious links or messages from unknown senders. However, their self-assessed understanding was often "somewhat good" or "limited," highlighting a gap between awareness and actionable knowledge. While some respondents had received formal training, many had not, revealing a lack of widespread digital safety education.

Table 3 - Experience with Phishing Attempts

Basis	Particulars	Frequency	Percentage
Clicked risky links or shared data unknowingly	Yes	10	18.2
	No	38	69.1
	Not sure	7	12.7
	Total	**55**	**100**
Likelihood of clicking links from unknown senders	Very Likely	3	5.5
	Somewhat likely	14	25.5
	Unlikely	16	29.1
	Never	22	40
	Total	**55**	**100**
Respondents' reaction to	Pause and verify the message	34	61.8
	Ignore it	8	14.5
	Act immediately	7	12.7

DOI: 10.48175/IJARSCT-26936

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 8, May 2025 Impact Factor: 7.67

panic/urgency in messages	Ask someone else	6	10.9
	Total	**55**	**100**

As shown in **Table 3**, responses to scenario-based questions revealed a mixed behavioral pattern. Many individuals claimed they would not click unknown links or respond to emotionally charged messages. However, a portion admitted they might act impulsively if an email appeared urgent or threatening. This demonstrates the ongoing effectiveness of social engineering tactics that exploit emotional triggers. A sizable number of participants responded that they would likely verify the message before acting, which is encouraging. However, a smaller—but significant—group still expressed acting immediately, highlighting lingering vulnerability

Table 4 - Behavioural Tendencies

Basis	Particulars	Frequency	Percentage
Targeted by phishing/ scams	Yes	36	65.5
	No	13	23.6
	Not sure	6	10.9
	Total	**55**	**100**
Response to urgent 'account freeze' scam emails	Call the bank directly	23	41.8
	Ignore the email	18	32.7
	Ask someone else for advice	10	18.2
	Click the link and follow instructions	4	7.3
	Total	**55**	**100**
	Reported it	34	65.4
	Ignored it	6	11.5
	Informed others	9	17.3
	Took no action	3	5.8
	Total	55	100
	Yes	36	65.5
	No	19	34.5
	Total	55	100
	Yes	31	56.4
	No	14	25.5
	Not sure	10	18.2
	Total	55	100

Table 4 shows that when asked about past encounters with phishing, over half the respondents confirmed receiving suspicious messages. Among those who realized they had been targeted, the majority reported taking corrective action—either by informing others, reporting the incident, or changing account credentials. This proactive behavior is a positive sign, where reporting rates exceeded 65%.

Nonetheless, regular preventive practices—such as enabling two-factor authentication or maintaining strong password hygiene—were not consistently followed. These gaps point to a need for reinforcing good cybersecurity habits, not only after incidents but as routine behavior.

The study also found that a significant number of respondents expressed a strong interest in receiving further awareness material, underlining a desire for continuous learning. This openness, combined with an emerging understanding of emotional manipulation, signals a positive direction for future awareness campaigns.

DOI: 10.48175/IJARSCT-26936

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

V. FINDINGS AND DISCUSSION

- 85.6% of respondents had heard of phishing. They could identify basic red flags (e.g., suspicious links, unknown senders). However, fewer , 32.7% , understood how social engineering works, especially emotional manipulation like impersonation, urgency, or fear tactics.
- 61.8% of participants reported they would verify suspicious emails before acting. A smaller group, 12.7%, admitted they might act impulsively if a message seemed urgent. This shows that emotional triggers can override awareness, especially under pressure.
- 65.4% of those respondents who identified a phishing attempt took corrective action: reporting the incident. 17.3% warned others and 11.5% ignored it. This indicates an increasing sense of responsibility and awareness once a threat is recognized.
- 56.4% of respondents used two-factor authentication and changed passwords regularly. 34.5% admitted to not following consistent safety practices like regular password updation. This gap shows that awareness doesn't always translate into everyday cyber hygiene.
- A large majority, 75.5%, expressed interest in learning more about phishing. This reveals a willingness to improve awareness, even among those who already feel somewhat informed. It presents an opportunity for targeted training programs that address both emotional and technical vulnerabilities.

To summarise:

- Knowledge is not always protective—emotions like fear can bypass caution.
- Action often follows exposure—people act after an incident, not always before.
- Awareness campaigns should focus on both emotional resilience and behavior change.

VI. RECOMMENDATIONS

- Include real-life phishing simulations that mimic urgency, fear, or authority manipulation in schools, colleges and workplaces, by using relatable and real - time examples. This helps the ordinary individual practice staying calm and verifying before acting on impulse.
- Create awareness for and encourage routine password changes, 2FA setup, and digital footprints of individuals on the internet. This helps keep their online identities secure from pretexting attempts.
- Make it easier for users to report phishing within platforms like – Gmail, Outlook, especially banking apps – if they see a suspicious message or scam attempt. This will simplify reporting channels, making it easier for those not well versed with technology to get help.
- Use proof and testimonials from incidents within society to show that cautious behavior is common and encourage sharing of scams incidents within the community to normalize skepticism among individuals.
- Use newsletters, pop-up messages, or alerts on digital platforms to inform people of fresh, ongoing scam types and reinforce this alertness through short, periodic reminders.

VII. CONCLUSION

This study set out to understand the susceptibility of individuals in Bengaluru, India, to phishing attacks that rely on social engineering. The results indicate that while general awareness about phishing is widespread, many individuals remain vulnerable due to emotional manipulation, limited formal training, and inconsistent preventive habits.

Most participants could recognize common technical signs of phishing, but fewer were equipped to respond calmly when faced with emotionally charged situations. Behavior under pressure revealed that even informed users could be persuaded by urgency or fear, underscoring the strength of social engineering tactics.

Importantly, the study also uncovered encouraging trends. Many respondents took action after encountering phishing, and a strong majority expressed interest in learning more. This shows not only a growing awareness of the risks, but a willingness to engage and improve.

Overall, the findings reinforce the need to move beyond surface-level awareness. Effective phishing prevention must include behavioral training, emotional resilience, and a culture of digital mindfulness. With the right tools and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, May 2025
Impact Factor: 7.67

consistent reinforcement, individuals can learn not only to recognize phishing—but to respond with clarity, confidence, and caution.

REFERENCES

[1]. Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

[2]. Butavicius, M., Parsons, K., Pattinson, M., & McCormac, A. (2021). Breaching the human firewall: Social engineering in phishing and spear-phishing emails. Computers in Human Behavior Reports, 3, 100072. https://doi.org/10.1016/j.chbr.2021.100072

[3]. Ferreira, A., & Lenzini, G. (2020). An analysis of social engineering principles in effective phishing. Human-centric Computing and Information Sciences, 10(1), 1–23. https://doi.org/10.1186/s13673-020-00236-5

[4]. Hijji, M., & Alam, G. (2021). A multivocal literature review on growing social engineering-based cyber-attacks during the COVID-19 pandemic: Challenges and prospective solutions. Computers & Security, 109, 102386. https://doi.org/10.1016/j.cose.2021.102386

[5]. Jansson, K., & von Solms, R. (2013). Phishing for phishing awareness. Behaviour & Information Technology, 32(6), 584–593. https://doi.org/10.1080/0144929X.2011.632650

[6]. Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Namin, A. S. (2020). How social engineers use persuasion principles during vishing attacks. Computers & Security, 92, 101748. https://doi.org/10.1016/j.cose.2020.101748

[7]. Team, C. (2024, December 9). Which Industries Are Most at Risk of Phishing Attacks?.

[8]. https://www.clickguard.com/blog/industries-most-at-risk-of-phishing-attacks

[9]. Woollacott, E. (n.d.). What is phishing? Understanding Cyber attacks. Forbes. https://www.forbes.com/sites/technology/article/what-is-phishing/

[10]. Desk, T. (2025, April 21). Gmail user? Beware of this sophisticated phishing attack. The Indian Express. https://indianexpress.com/article/technology/tech-news-technology/gmail-sophisticate d-phishing-attack-9954939/

[11]. Sharma, D. (2024, April 30). India recorded over 79 million phishing attacks in 2023, new study suggests. India Today. https://www.indiatoday.in/technology/news/story/india-recorded-over-79-million-phis hing-attacks-in-2023-new-study-suggests-2533497-2024-04-30