# Clicking on Danger: Ranking Cyber Threat Factors and the Protective Role of Awareness

Hissan Kibria,
*Cadet College Hasanabdal*
Imran E. Kibria,
*Ohio State University*

## Abstract

SMS Phishing (SMShing) attack is the act of sending messages containing malicious links that cause malware or breach data. Cyber criminals conduct these attacks by leveraging psychological factors, including Urgency, Fear, Curiosity, and Trust. These attacks have become prevalent in Pakistan, and research into responsible factors can help strengthen security infrastructure. In this study, we order the four psychological factors in order of their potency, analyze the effect of SMiShing literacy, and draw safety measures for security. We surveyed 200 college students and concluded that Fear and Urgency are potential factors behind engaging in malicious messages.

## Introduction

SMiShing (SMS Phishing) is one of the most notorious types of Phishing Attacks. It uses social engineering to trick people into entering sensitive and private information on malicious websites. The URLs of websites or malware software are part of text messages sent by cyber criminals with the intent of privacy invasion. These cyber criminals craft messages that appear legitimate, as if sent from an official organization, to create an illusion of legitimacy. However, their true purpose is breaching data for personal benefit.

This study will focus on the causes and effects of SMiShing attacks on the population of Pakistan. We will investigate four emotional factors including urgency, fear, curiosity, and trust to understand which of these factors makes Pakistan's youth most vulnerable to Smishing attacks. This understanding will in turn be helpful to training the young workforce in information security, thereby strengthening the nation's cybersecurity infrastructure (Daudi, 2024. vol. 3, no.2). Furthermore, our study will include how awareness on SMiShing can reduce its harmful effects. Lastly, we will draw necessary precautions and include government instructions to prevent Smishing attacks.

Our research is related to existing works in the literature. Many of these works investigate reasons why people engage with malicious messages. The study by a software firm, PhishFirewall, reported that fear and curiosity are the primary reasons for engaging with malicious texts. Blancaflor et al. pointed to the presence of curiosity and trust in the deception strategies of hackers (Rowles, August 5, 2024). These studies separately identified two factors each, amongst which curiosity was common. The study by Crumbaugh et al. (Crumbaugh, 2024) then investigated all three factors including curiosity, trust, and fear. Whereas, White et al. (Montgomery) investigated four causes of clicking on malicious links which included urgency, fear, curiosity, and trust to deceive the targets. Our study extends their research to rank these four factors in order of potency, analyze how awareness impacts engagement with malicious links, and draw preventive measures for safety. A relevant study to ours is that of Rehman et al. (Muhammad Lutfor Rehman, 2023) in which they studied about awareness, behavior, and experiences of college students with SMiShing and found that urgency and fear-based messages duped students.

Our survey will be focused on Pakistan's population because of the country's unique circumstances. Pakistan stands at Tier-1 in the ITU-Global Cybersecurity Index (GCI-V5) 2024 (Dawn, 2023), however numerous Smishing incidents are reported quite frequently. The National Telecommunications and Information Security Board identified a spoofed website of the State Bank asking for personal credentials of people. Criminals gained trust of their audience through call cloning, duplicating original logos, and mass spamming via SMS (Short Message Service) (Division, September 8, 2023). Similarly, a package delivery scam, supposedly from the Pakistan Postal Office, was identified by the NCERT Advisory. Criminals sent SMS to people threatening them with cancellation of package delivery if they did not provide their correct residential address (Division, September 8, 2023). This increased practice of invading privacy through cyber espionage or compromising user location are listed as information threats by the Government of Pakistan. More recently, criminals are taking advantage of VoIP (Voice over Internet Protocol) services, so their live location remains hidden, thus making it difficult for security officers to catch them. They threaten their audience with financial loss or fabricate a sham lawsuit to gain urgent attention. The widespread prevalence of such Smishing incidents indicates a need for research to identify causes and preventive measures in Pakistan.

Since the loss to Smishing attacks is largely unreported in Pakistan, we mention a few statistics from the United States to highlight the threat of Smishing Attacks. These attacks have surged by 328% in 2020 (Keepnet, 2025), and by 700% in the first half of 2021 (Office, 2024), with only 36% of the national population aware of SMiShing (Cooke, 2024). In a report from the Internet Crime Complaint Center, the Federal Bureau of Investigation documented over $3 million in losses (Jovanovic,

2021). 76% of the businesses were subject to SMiShing attacks, which later reported to have suffered significant financial loss as well (Keepnet, 2025).

## Results

In the first set of results, we rank four possible causes of Smishing, including urgency, fear, curiosity, and trust in order of their potency. Our survey of 200 Pakistani participants showed that 84 participants (42%) clicked on fear-based SMiShing messages, 64 participants (32%) responded to urgency-driven messages, 37 respondents (~19%) engaged with trust-based messages, and only 16 participants (8%) responded to curiosity-based messages. Hence, fear and urgency are the major factors that make Pakistan's youth susceptible to Smishing attacks. This is followed by trust and then curiosity. A low susceptibility to curiosity-based messages suggests that teenagers in Pakistan are less likely to fall for giveaways or easy money scams.

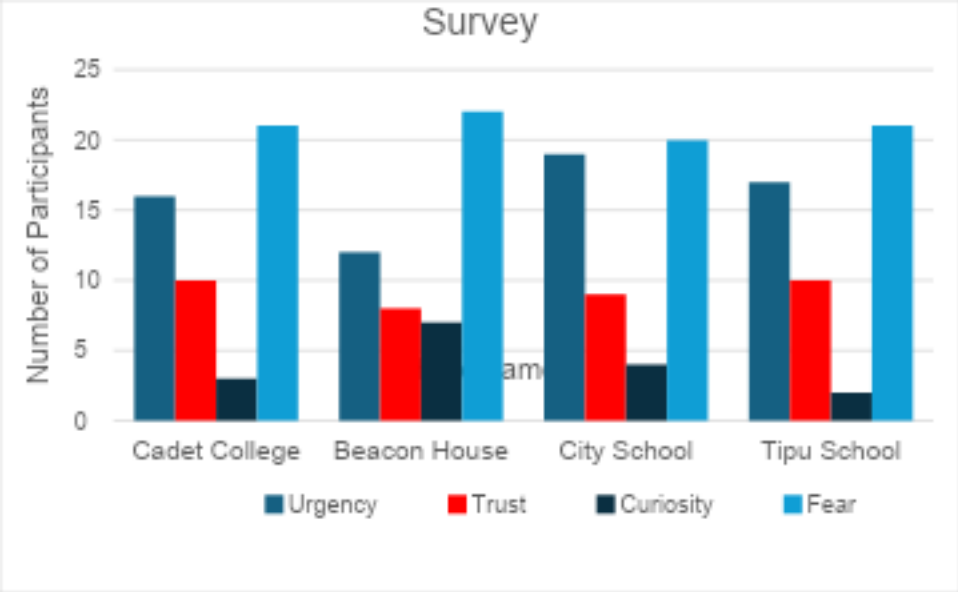


FIGURE 1. Column graph showing the number of participants from four schools: Cadet College, Beacon House, City School, and Tipu School, who identified specific emotional triggers—Urgency (blue), Trust (red), Curiosity (dark blue), and Fear (yellow)—as effective.

In the second set of results, we observe that individuals with prior knowledge of phishing attacks or experience with scams in the past were least likely to engage with Smishing-based messages. 27 of 200 participants in our survey were either aware of the term SMiShing or had faced it but just didn't know the exact terminology for it. However, the remaining participants were ignorant of Smishing. We compare the

engagement of both aware and unaware participants pictorially at the bottom of this document. Figure-2 is a pie chart corresponding to aware participants, depicting the ratio of people who clicked on malicious URLs versus those who remained safe. Whereas Figure-3 is a pie chart corresponding to unaware participants depicting the same division. A comparison of these figures demonstrates the positive impact of awareness.

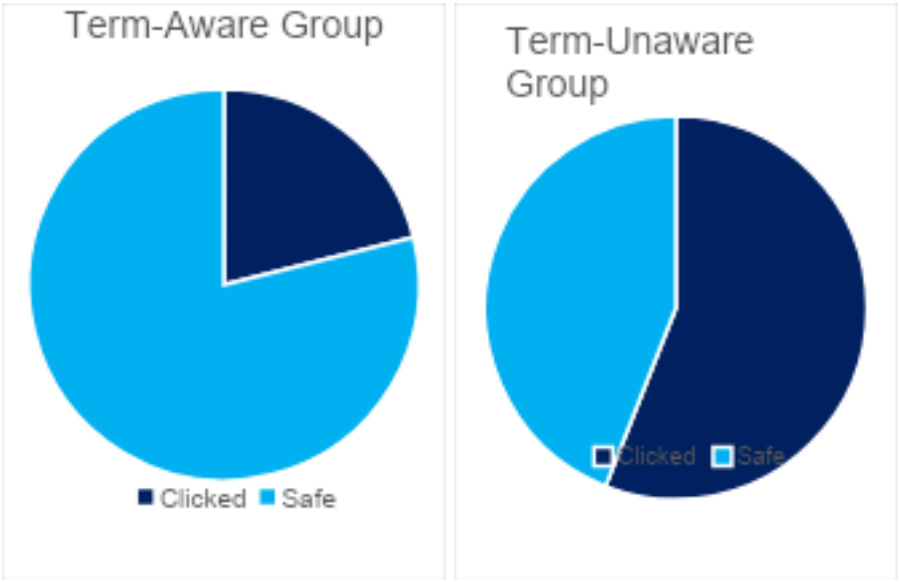


FIGURE 2 (LEFT) AND 3 (RIGHT). Pie Graph illustrating the ratio of those who clicked (Dark Blue) on the malicious link vs those who did not (Light Blue) in both groups: Term-Aware & Term-Unaware.

Finally, we have drawn preventive measures and precautions based on our survey findings, which we elaborate in the Discussion section.

## Discussion

The prompt of our trust-based messages is related to a phony reward, and it is frequently identified as a scam. This indicates that our surveyed population is not gullible and aware of manipulative tactics to a reasonable extent. Surprisingly, curiosity is identified as the most benign of all four factors, which is contrary to our expectations since the general perception of young people is that of being curious. We delineate on our message prompts relating to fear, urgency, trust, and curiosity in the Materials and Methods section.

Most of the students in the survey came from Semi-Urban or Urban backgrounds with a relatively higher cyber literacy and convenient access to the Internet. While interpreting the conclusions of the Research, it

should be noted that the findings reflect the privileged segment of Pakistan and should not be generalized to other regional or national contexts.

The strategies acquired by Hackers are not fixed; and continuously evolve in response to the increased awareness, firewalls and advancement in the technology. Thus, the findings of this study represent a snapshot in time and may not adhere or capture emergent tactics in Smishing. Future research in this regard should consider a longitudinal approach and monitor differences in Smishing tactics in different applications (WhatsApp, E-mail, Instagram). They may work alongside cybersecurity firms to monitor real-time attacks and study how they evolve in response to regulatory changes or technological advancements.

It should also be recognized that the responses of the survey highlight the cultural traditions and norms like: High respect for authoritative personnel or their commands, collective family decision-making, limited exposure to digital literacy and lack of 24/7 Internet access. Such cultural factors might have influenced the high response rate for Fear and Urgency.

We list necessary precautions for safety from such SMiShing attacks based on our findings:

1. Treat unsolicited messages with skepticism. Remain cautious in interaction if you are being asked for personal information since legitimate sources do not reach out for these details. In exceptional scenarios like identity verification, personal information may be asked but it is never required to text this information since it violates standard privacy practices.
2. Avoid directly clicking on links to open a webpage. If a link is sent via a message and you are required to open that web page, avoid directly clicking on it. Instead, prefer to copy the link into a search engine. Remove a few letters/digits/symbols from the end of the link and then click enter. You will not be directed to your intended website, but many relevant search results will show. Now, if the original link is indeed authentic, it will likely be one of the top results.
3. Use security software in mobile phones. Security software always defends devices against many threats while executing in the background. There exist many renowned software applications for protection, some of which are free while others require subscription. Softwares could be Anti-viruses, Anti-Malwares, or Anti-Spywares.
4. Digital and Cyber literacy should be made part of school curricula. Awareness about such Cyber-attacks (Inclusive Smishing) should be given from a young age. Programs like Junior Cyber Superheroes, of PKCERT, should be integrated in the Computer Science syllabus and appropriately tested. Early education regarding digital safety helps one to develop life-long habits for privacy protection. Education ministers and digital

security agencies should collaborate for aligning school curricula with cyber safety policies.

In addition to preventive measures, we list governmental measures proposed in this regard.

National Cyber Security Policy, 2021 outlines a comprehensive framework for protecting critical information infrastructure, enhancing cyber security governance, and promoting public-private partnerships (Pakistan D., 2021). Under the Prevention of Electronic Crimes Act, 2016 phishing and SMiShing are declared illegal, and regulations are implemented (Pakistan G. O.). Advisory No. 54 issued by National Telecom and Information Technology (NTISB) specifically addresses spear phishing attacks targeting Pakistan's sensitive information ((NTISB), Cyber Security Advisory Secure Email Communications (Advisory No. 54), 2023). In addition, the government has established Cyber Emergency Response Teams (CERTs) for quick real-time responses to cyber threats. Regulatory bodies like the Pakistan Telecommunication Authority (PTA) also actively work on filtering and blocking malicious websites, making it safe for non-technical individuals to surf the web.

While much of the current discourse on SMiShing and mobile security draws from technical or cybersecurity perspectives, this study also recognizes digital literacy as a socio-technical phenomenon. As STS scholars such as Selwyn (Selwyn, 2010) and Lupton (Lupton, 2017) argue, digital literacy is not just a matter of skills, but is shaped by broader sociocultural practices, power dynamics, and access to technology. This framing is particularly relevant in the Pakistani context, where digital divides and infrastructural constraints influence how people interact with mobile technologies.

## Materials and Methods

In this section we delineate on cyber threat factors including urgency, fear, curiosity, and trust. Then we elaborate on details of our surveyed population, mode of data collection, and prompt message corresponding to each factor. Our message prompts are designed to mimic cyber-criminal behaviors. As previously noted, cyber criminals will pretend to be affiliated with well-renowned organizations including banks and federal institutes to appear legitimate. They will refer to themselves as the institute's representative and manipulate a recipient into providing sensitive data. Their motivation can be selling this data to the highest bidder on the dark web.

The four psychological factors influencing teenagers in becoming victim to Smishing attacks include urgency, fear, curiosity, and trust. Urgency is the sense of needing to act quickly to avoid loss. It works by creating tension in an individual and prompting involuntary impulsive actions that frequently result in long-term loss. Fear is the sense of operating under threat. It dominates the consciousness of the brain and

manipulates recipients into entering sensitive information. Fear-based manipulation can be threatening with account termination or other financial loss. Curiosity is the sense of exploring new avenues to learn their outcome. Teenagers are inherently curious and free access to the latest iPhone, or a new gaming PC incites them to act. Lastly, trust is the sense of acting without any skepticism. Recipients respond without critically evaluating malicious SMS because they are under the false impression of institutional legitimacy. In the following sections we exemplify each of the four factors.

1. *Urgency:* It is observed that almost every Smishing attack urges quick response from recipients. It is because the malicious web links are tracked and shut down in a short time, hence cyber criminals only have a short time window to leverage. They typically ask users to act in the moment or on a short notice due to fear of the website being taken down. Between 2019 and 2020, a dramatic 475% increase in SMiShing attacks relying on creating urgency in victims was reported (KnowBe4, 2024).
2. *Fear:* Cyber criminals exploit gullible people by sending alarming texts to create a sense of fear. In the study by Hamid Wali et al., 16.92% of participants were reported to fall victim to fear-based SMiShing attacks where recipients did not even verify the authenticity of received messages (Muhammad Lutfor Rehman, 2023). In Pakistan, groups of hackers including the "SMiShing Triad" that impersonated the Pakistan Post, also conducted fear-based attacks to obtain credentials of victims (Paganini, 2024).
3. *Curiosity:* Hackers leverage the weak points of individuals and systems. Young people are inherently curious, delving into everything they find rewarding. Tomer Shloman et al. have highlighted that phishers use curiosity-inducing content such as exclusive offers, intriguing content, and special discounts (Shloman, 2024). Similarly, in a recent SMiShing case in Pakistan, attackers sent WinRAR zip files to users, instructing them to unzip the file to claim a reward, ultimately delivering malware.
4. *Trust:* A study conducted in 2023 indicated that nearly 60% of the teenagers who fall victim to a SMiShing attack trusted it to be from a credible and legitimate source (Eventus Security, 2024). Trust becomes the basis for young people to enter their sensitive information on malicious websites. In 2023, spoof websites of the Army Poverty Alleviation Campaign and the Revival of Economy Campaign were used to trick victims into uploading their financial details, resulting in a loss to thousands of people ((NTISB), Cyber Security Advisory – Prevention

Against Financial Scam Activities – Impersonation as Govt Officials, 2023).

## Methodology

We conducted a survey of 200 young people in Pakistan from four different colleges. Our sample size may be small and Urban-Pakistan based which may not accurately represent the entire youth population of Pakistan, especially the underserved areas. However, it provides valuable insights regarding susceptibility to SMiShing among cyber-literate youth in urban Pakistan.

All teenagers surveyed were between 10th and 12th grade, aged between 13 and 19 years. Of the 200 participants, 112 (56%) were male and 88 (44%) were female, the gender ratio of males was slightly higher than females since one of the four colleges is an all-boys institute. All participants were from the following four colleges: Cadet College Hasanabdal, Beacon House School system, The City School, and Tipu School. These institutions are in the Rawalpindi division in Pakistan.

Our data is collected both online via Google Survey form and in-person using printed questionnaires. The instructions were straightforward. (1) They were asked to choose their background from the following categories: Rural, Sub-Urban, Urban, (2) their school/college grade, (3) their gender, (4) a Yes/No question if they were aware of the term Smishing and lastly (5) they were presented with message prompts (as shown later) containing malicious URLs and asked to select which message they would most likely engage with. Each survey only took between two and five minutes of a student. The participants were recruited on a random-basis and nearly every student was willing to take part in the research. We also asked for permission to record and present responses for research purposes.

We generated prompts corresponding to each threat factor by using an AI tool called Copilot. These prompts are shown below. In our instructions, we additionally asked Copilot to mimic the behavior of cyber criminals. After the AI generated the prompts, we compared them to real-world Smishing messages from publicly available databases (OpenPhish, Cofense Email Security, Kaggle). Once we evaluated the realism of Message Prompts, we took it to one of the representatives of PKCERT to verify its authenticity. Minor adjustments were made and the following prompts were finalized.

Urgency-based Prompt: The sender was supposedly the Allied Bank. The prompt read, “Your account has been temporarily suspended due to suspicious activity. You must verify your identity within the next 30 minutes to avoid permanent deactivation. Click here: [malicious link]".

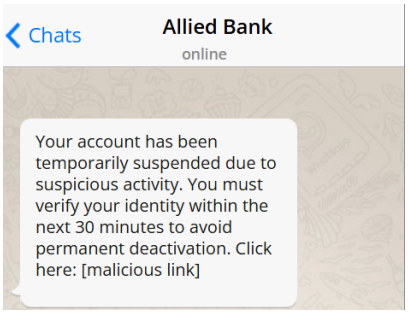


FIGURE 4. Urgency-Based Prompt.

Trust-based Prompt: The sender was supposedly the Edhi Centre. The prompt read, “You are eligible for a free COVID-19 relief fund of PKR 10,000. Claim your payment securely by verifying your details here: [malicious link]. Failure to verify will result in fund expiration."

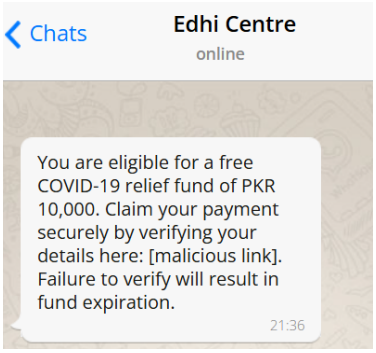


FIGURE 5. Trust-Based Prompt.

Curiosity-Based Prompt: The sender was supposedly the TV show named Jeeto Pakistan. The prompt read, "Congrats! 🎉 Your number was randomly selected for an exclusive giveaway. You have won a brand-new iPhone 15! 🎁 Claim now before your prize is given to the next winner: [malicious link]"

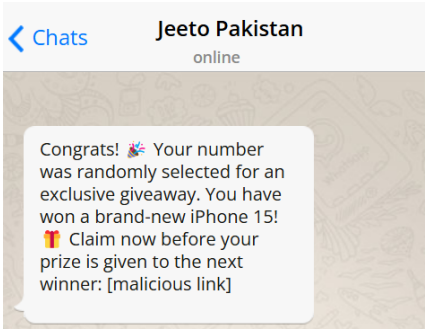


FIGURE 6. Curiosity-Based Prompt.

Fear-based Prompt: The sender was supposedly the Punjab Police. The prompt read, "A case has been registered against your CNIC for illegal financial activity. Immediate legal action will be taken unless you verify your identity here: [malicious link]. Respond within 2 hours to avoid arrest."

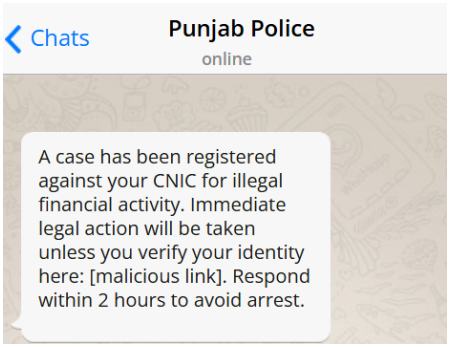


FIGURE 7. Fear-Based Prompt.

## References

Alarcón, D., Sánchez, J. A. & De Olavide, U. (2015). Assessing convergent and discriminant validity in the ADHDR IV rating scale: User-written commands for Average Variance Extracted (AVE), Composite Reliability (CR), and Heterotrait-Monotrait ratio of correlations (HTMT) (pp. 1-39). Spanish STATA Meeting, Vol. 39.

(NTISB), N. T. (2023). Cyber Security Advisory – Prevention Against Financial Scam Activities – Impersonation as Govt Officials. Cabinet Division of the Government of Pakistan.

(NTISB), N. T. (2023). Cyber Security Advisory Secure Email Communications (Advisory No. 54). Cabinet Division of the Government of Pakistan.

Cooke, T. (2024, July 2). Earthweb. 13+ Smishing Statistics in 2025 (SMS Phishing Attacks).

Crumbaugh, J. (2024, April 18). Understanding Social Engineering: Staying Safe from Human-activated Threats. Phish Firewall.

Daudi, M. (2024. vol. 3, no.2). Exploiting Human Trust in cybersecurity: Which Trust Development Process is Predominant in Phishing Attacks? ACIG, 233-249.

Dawn. (2023, December 21). Pakistan Among Top Countries in Cybersecurity: IT Minister.

Division, C. (September 8, 2023). Cyber Security Advisory – Prevention Against Financial Scam Activities - Impersonation as Govt Officials (Advisory No. 53). National Telecommunications and Information Security Board.

Eventus Security. (2024). Smishing Triad Targets Pakistan with Malicious Messages Exploiting User Data.

Jovanovic, A. (2021, May 18). SafetyDetectives. 10 Facts + Stats on

Smishing (SMS Phishing) in 2025.
Keepnet. (2025, January 26). Smishing Statistics 2025: The Latest Trends and Numbers in SMS Phishing.
KnowBe4. (2024). Phishing.
Lupton, D. (2017). Digital Sociology. Liverpool: Routledge.
Montgomery, C. (n.d.). Throttlenet. 6 Ways to Prevent Treacherous Smishing Attacks.
Muhammad Lutfor Rehman, D. T. (2023). Users really do respond to smishing. In Proceedings of ACMConference (CODASPY'23).
ACM, (p. 15). New York, USA.
Office, I. S. (2024, February 29). Computing Services - News. Stay Alert for Fraudulent Text Messages.
Paganini, P. (2024, June 20). Security Affairs. SMiShing Triad Is Targeting
Pakistan to Defraud Banking Customers at Scale.
Pakistan, D. (2021). National Cybersecurity Policy 2021. Ministry of Information Technology and Telecommunication.
Pakistan, G. O. (n.d.). The Pakistan Code: With Chronological Table and Index. Karachi: Karachi: Manager of Publications.
Rowles, R. (August 5, 2024). Unmasking Emotional Triggers in Social Engineering Attacks. Security Boulevard.
Selwyn, N. (2010). Looking beyond learning: Notes towards the critical study of educational technology. Journal of Computer Assisted Learning, 65-73.
Shloman, T. (2024, February 1). Trellix. The Psychology of Phishing: Unraveling the Success Behind Phishing Attacks and Effective Countermeasures.