Smishing in Pakistan

Sara Malik
PakCrypt Organization
smk@pakcrypt.org

***Abstract*— Smishing, or SMS phishing, has emerged as a significant cybersecurity threat in Pakistan, leveraging the widespread use of mobile phones to deceive users into divulging sensitive information. This paper examines the prevalence of smishing attacks in Pakistan, highlighting notable incidents and analyzing the factors contributing to their rise. Through a survey of reported cases and existing literature, we identify key vulnerabilities within Pakistan's digital landscape. The analysis underscores the role of limited public awareness, inadequate regulatory measures, and technological challenges in exacerbating smishing threats. To mitigate these risks, we propose potential solutions at both individual and governmental levels, including enhanced cybersecurity education and stronger policy enforcement. The findings aim to inform stakeholders and contribute to the development of effective strategies to combat smishing in Pakistan.**

Keywords—smishing, cyber-security, cyber-awreness, financial fraud, cyber-crime (*key words****)***

I. Introduction

Smishing, a blend of "SMS" and "phishing," refers to fraudulent activities where attackers use text messages to trick individuals into revealing personal information such as passwords, credit card numbers, or other sensitive data. As mobile phone usage has surged globally, smishing has become a prevalent cyber threat, exploiting the trust users place in their personal devices.

In Pakistan, the rapid increase in mobile phone penetration has made the population particularly vulnerable to smishing attacks. According to the Pakistan Telecommunication Authority (PTA), there are over 180 million mobile subscribers in the country, creating a vast target pool for cybercriminals. Several notable incidents have highlighted the severity of the issue:

- Fake Prize Schemes: Attackers send messages claiming the recipient has won a lottery or prize from a well-known company, requesting personal details or a processing fee to claim the reward.
- Banking Scams: Fraudulent texts purporting to be from banks ask customers to verify their account information due to a security issue, leading to unauthorized access to their accounts.
- COVID-19 Relief Fraud: During the pandemic, messages offering financial aid or vaccines were used to harvest personal data from concerned citizens.

These incidents underscore the pressing need for increased awareness and robust measures to protect individuals from smishing threats in Pakistan.

II. Related Research

In recent years, smishing has attracted considerable attention from researchers aiming to understand and mitigate its impact. Key areas of focus include detection techniques, user behavior analysis, and prevention strategies. Notable studies and findings in the last five years include:

- Detection Methods: Researchers have explored machine learning algorithms to identify smishing messages by analyzing linguistic patterns and message metadata. Techniques such as natural language processing (NLP) and artificial intelligence (AI) have shown promise in differentiating between legitimate and fraudulent messages.
- User Awareness Studies: Surveys conducted in various regions, including South Asia, reveal a general lack of awareness about smishing among mobile users. Educational interventions have been proposed to enhance user recognition of potential threats.
- Cultural and Regional Analysis: Studies specific to developing countries highlight how socio-economic factors contribute to the susceptibility of individuals to smishing attacks. Limited digital literacy and trust in authoritative messages increase the effectiveness of such scams.

Given the evolving nature of smishing tactics, ongoing research is crucial. For comprehensive insights, reviewing recent publications in cybersecurity journals and conference proceedings is recommended.

III. Survey of Smishing Incidents in Pakistan

Smishing, a form of phishing conducted via SMS, has emerged as a significant cybersecurity threat in Pakistan. Cybercriminals exploit this technique to deceive individuals into divulging sensitive information, such as personal and financial details. This survey examines reported smishing incidents in Pakistan, drawing from news articles, cybersecurity publications, and government advisories.

A. Smishing Triad Targeting Pakistani Banking Customers

In June 2024, cybersecurity firm Resecurity identified a campaign by the "Smishing Triad," a cybercriminal group that expanded its operations to Pakistan. The group impersonated Pakistan Post, sending malicious messages via iMessage and SMS to customers of major mobile carriers, including Jazz/Warid, Zong, Telenor Pakistan, and Ufone. The objective was to steal personal and financial information by directing recipients to phishing sites mimicking official Pakistan Post websites. The attackers sent between 50,000 to 100,000 messages daily, leveraging stolen databases containing citizens' phone numbers. [1]

B. Expansion of Smishing Triad's Activities

Further analysis by CyberMaterial highlighted the Smishing Triad's sophisticated tactics, including the use of local phone numbers to enhance the credibility of their messages. The group also impersonated other courier services like TCS, Leopard, and FedEx, luring victims with claims of undelivered packages or urgent account issues. This activity began in May and peaked in June 2024. [1]

C. Government Advisory on Smishing Threats

The National Cyber Emergency Response Team of Pakistan (PKCERT) issued a security advisory in response to the rising smishing incidents. The advisory urged citizens to be cautious of unsolicited messages requesting personal information and provided guidelines to protect against such scams. Telecom operators were also advised to enhance their fraud detection systems to proactively block malicious activities.[1]

D. Historical Context and Rising Trends

Smishing attacks have been a growing concern globally. A report by Kroll in August 2022 noted that smishing attacks were reported in 74% of companies in 2021, up from 61% in 2020. Initially, these attacks impersonated banks and financial services but later expanded to package delivery services, a trend observed in Pakistan with the Smishing Triad's activities.[2]

E. Public Awareness and Reporting

Public awareness has been crucial in combating smishing. Reports on platforms like Reddit have shown that users shared experiences of receiving suspicious messages, prompting discussions on identifying and avoiding such scams. Cybersecurity firms and media outlets have also played a role in educating the public about the nature of smishing attacks and preventive measures.[3]

IV. Detailed Analysis

There are several factors contributing to the proliferation of Smishing attacks in Pakistan. The rise in smishing attacks in Pakistan is attributed to a combination of technological, social, and regulatory factors. Below is a detailed analysis of these contributing factors:

A. High Mobile Penetration and Digital Adoption

Mobile Usage: Pakistan has a high penetration of mobile phones, with over 80% of the population owning a mobile phone, and a significant proportion using smartphones. This widespread adoption creates a large target pool for attackers.
SMS Reliance: Many services, including banking, e-commerce, and courier services, rely heavily on SMS for communication, making it a familiar and trusted medium.
Increased Internet Usage: With rising internet adoption and digital services, users are engaging more online, providing attackers with more avenues to exploit.

B. Lack of Public Awareness

A large portion of the population lacks awareness about cybersecurity threats, particularly smishing. This makes users more susceptible to falling for fraudulent messages. Citizens often trust SMS claiming to be from banks, courier companies, or government agencies, without verifying the authenticity.

C. Awareness Weak Data Protection Regulations

Data Breaches and Leaks: Frequent incidents of data breaches expose personal information such as phone numbers, making it easier for attackers to target individuals.
Limited Regulation Enforcement: Pakistan has data protection laws, such as the Personal Data Protection Bill 2020, but enforcement remains weak, allowing attackers to operate with minimal consequences.
Unregulated Telecommunication Sector: Fraudulent SMS often originate from local numbers or spoofed identities due to inadequate monitoring and control mechanisms in telecom networks.

D. Sophisticated Cybercriminal Operations

Use of Localized Strategies: Attackers, like the Smishing Triad, exploit local languages, cultural nuances, and popular brands (e.g., Pakistan Post, TCS) to make their messages more convincing.
Technological Sophistication: Cybercriminals employ advanced tools to automate the sending of thousands of messages daily, using local number spoofing and phishing websites that mimic legitimate platforms.
Shift in Tactics: Initially focused on banks, attackers have expanded to target courier services and government organizations, increasing the diversity of scams.

E. Financial Incentives for Attackers

High Return on Investment: Smishing is a low-cost and high-reward tactic. With minimal resources, attackers can extract significant financial and personal data from victims.
Access to Global Markets: Pakistan's integration into global networks means stolen data can be monetized or sold on international dark web platforms.

F. Insufficient Telecom Security Measures

Inadequate Screening: Telecom companies often lack robust mechanisms to filter and block malicious messages effectively.
SIM Cloning and Fraud: Pakistan has faced issues with SIM fraud, which facilitates smishing by allowing attackers to impersonate legitimate entities.

G. Pandemic-Induced Shift to Digital Platforms

Increased Digital Activity: The COVID-19 pandemic accelerated the shift to online transactions and communications, increasing reliance on SMS-based authentication and updates.
Exploitation of Pandemic-Related Themes: Attackers leveraged themes such as vaccine registrations and government aid disbursements to deceive users.

H. Social Engineering Exploits

Emotional Manipulation: Messages often use urgency ("Your package is stuck!") or fear ("Your account will be blocked!") to prompt immediate, irrational responses.
Lack of Verification Behavior: Many users do not cross-check information or contact service providers to validate claims in suspicious messages.

I. *Inconsistent Government Interventions*

Delayed Response to Emerging Threats: Authorities have been slow in issuing public warnings or prosecuting cybercriminals effectively.
Limited Public Campaigns: While some advisories have been released, there is a need for broader, sustained efforts to educate citizens about smishing risks.

J. *Cross-Border Cybercrime Networks*

Global Smishing Campaigns: Groups like the Smishing Triad operate across multiple countries, exploiting weak cybersecurity measures in developing nations like Pakistan.
Challenges in International Cooperation: The global nature of these crimes makes it difficult for local authorities to track and prosecute perpetrators based abroad.

V. Potential Solutions

A. *Individual Level*

- Education and Awareness: Launch campaigns to educate the public about smishing, how to recognize it, and steps to take when receiving suspicious messages.
- Vigilance: Encourage individuals to verify the authenticity of messages by contacting organizations directly through official channels.
- Security Practices: Promote the use of mobile security applications and advise against sharing personal information via SMS.

B. *Government Level:*

- Strengthen Regulations: Enhance laws pertaining to cybercrime, specifically addressing smishing, with clear penalties.
- Improve Enforcement: Allocate resources to law enforcement agencies for better detection, investigation, and prosecution of cybercriminals.
- Collaboration with Telecom Operators: Mandate telecom companies to implement advanced filtering systems to detect and block smishing messages.
- Public-Private Partnerships: Foster collaboration between government, private sector, and NGOs to develop comprehensive strategies against smishing.
- Reporting Mechanisms: Establish and promote accessible channels for reporting smishing incidents, aiding in data collection and response efforts.

VI. Conclusion

Smishing poses a significant threat to individuals and the broader economic stability in Pakistan. Addressing this issue requires a multifaceted approach involving increased public awareness, stronger regulatory frameworks, and technological advancements in detection and prevention. By taking concerted action at both individual and governmental levels, Pakistan can reduce the impact of smishing and enhance its overall cybersecurity posture.

References

[1] https://www.resecurity.com/blog/article/smishing-triad-is-targeting-pakistan-to-defraud-banking-customers-at-scale?utm_source=chatgpt.com

[2] https://www.kroll.com/en/insights/publications/cyber/monitor/vishing-smishing-attacks?utm_source=chatgpt.com

[3] https://www.hackread.com/chinese-smishing-triad-group-pakistan-sms-phishing/?utm_source=chatgpt.com

[4] Nahapetyan, Aleksandr, et al. "On sms phishing tactics and infrastructure." 2024 IEEE Symposium on Security and Privacy (SP). IEEE Computer Society, 2024.