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 13, April 2025
Impact Factor: 7.67

Mobile Device User's Susceptibility to Phishing Attack

Asst. Prof. Shradha Wankhede[1], Asst. Prof. Priyanka Choudhary[2], Mr. Prem Mangrulkar[3]
Assistant Professor, Dept. of Computer Science & Engineering[1,2]
Under-Graduate Student, Dept. of Computer Science & Engineering[3]
Tulsiramji Gaikwad Patil College of Engineering and Technology, Nagpur, India
shradha.cse@tgpcet.com, priyankaghotekar22@gmail.com, premmangrulkar22@gmail.com

Abstract: *As mobile devices become the primary gateway to digital communication and online services, they have also emerged as a major target for phishing attacks. This research explores the susceptibility of mobile device users to phishing attempts, highlighting the factors that contribute to their vulnerability. Unlike traditional computer users, mobile users often face unique challenges, such as smaller screen sizes, simplified interfaces, and limited access to security tools, which make it harder to detect malicious links or fake websites. Through a combination of user surveys, case studies, and an analysis of recent phishing trends, this study identifies key behavioural, technical, and psychological factors that increase the likelihood of falling victim to such attacks. The findings emphasize the need for improved user awareness, adaptive mobile security mechanisms, and better design practices to minimize risk. This paper aims to contribute to the ongoing efforts in enhancing mobile cybersecurity and protecting users from evolving phishing tactics.*

Keywords: Mobile Security, Phishing Attacks, Smishing, Cybersecurity Awareness, User Behaviour, Mobile Device Vulnerability, Social Engineering, Mobile Threats, Information Security, Human Factors in Cybersecurity.

I. INTRODUCTION

In today's digitally connected world, mobile devices have become an essential part of daily life. From online banking and shopping to social networking and email, smartphones and tablets are used to access a wide range of services on the go. However, this growing reliance on mobile technology has also made users increasingly vulnerable to cyber threats—particularly phishing attacks. Phishing, a deceptive tactic used to trick individuals into revealing sensitive information, has evolved beyond emails to exploit SMS (smishing), social media, and even mobile apps.

Unlike desktop environments, mobile platforms often present limited visual cues that could help users detect suspicious content, such as full URLs or security warnings. Additionally, users are often multitasking or in a hurry when using mobile devices, which can lead to careless clicking and reduced scrutiny of messages or links. These factors contribute to a higher risk of falling prey to phishing attempts on mobile platforms.

DOI: 10.48175/IJARSCT-26008

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 13, April 2025
Impact Factor: 7.67

This paper investigates the susceptibility of mobile device users to phishing attacks by examining current trends, user behaviours, and platform limitations. By identifying key risk factors and gaps in awareness, this study seeks to provide actionable insights for improving mobile cybersecurity practices and user education.

Key features of this study include:

- Analysis of phishing techniques tailored specifically for mobile platforms.
- Survey-based insights into user awareness, behaviour, and response to phishing attempts.
- Evaluation of mobile operating systems' built-in security mechanisms and their effectiveness.
- Recommendations for improving mobile cybersecurity through user education and app design.
- By examining both the human and technical sides of the issue, this study provides a comprehensive look at why mobile users are at risk and how these risks can be mitigated.

II. LITERATURE REVIEW

The growing reliance on mobile devices has attracted the attention of cybersecurity researchers, especially as phishing attacks continue to evolve and target mobile users more aggressively. Several studies have explored how the unique characteristics of mobile platforms contribute to increased vulnerability.

According to Kumar and Rathore (2020), mobile users are more likely to fall for phishing attacks due to reduced visibility of full URLs and a general lack of in-depth browser features that could help detect malicious content. Their findings suggest that the smaller screen size and simplified layouts on mobile devices can obscure important indicators of legitimacy, such as HTTPS certification or domain names.

In another study, Alsharnouby, Alaca, and Chiasson (2015) emphasized the role of user behaviour in phishing susceptibility. They found that users often do not scrutinize links or messages carefully—especially on mobile devices where multitasking is common and attention spans are shorter. The convenience of quick actions on smartphones can result in impulsive clicking, increasing the risk of falling victim to phishing schemes.

Additionally, the work of Engelman et al. (2016) pointed out that mobile apps and SMS-based attacks (commonly referred to as "smishing") are rapidly becoming preferred methods for attackers. These platforms often bypass traditional email filters and security systems, reaching users more directly and personally.

Moreover, research by Zhang and McDowell (2019) highlights that users' lack of cybersecurity awareness significantly impacts their vulnerability. Many mobile users remain unaware of the tactics used by attackers or fail to recognize red flags, such as suspicious links or urgent language designed to create panic and prompt immediate action.

Finally, recent literature has explored technical solutions, such as browser warning systems, mobile antivirus tools, and AI-driven phishing detection (Gupta et al., 2021). While these tools show promise, they are not foolproof, especially when user behaviour undermines their effectiveness.

In summary, the existing body of research underscores that mobile phishing is a multifaceted threat driven by both technical limitations and human factors. The combination of minimal screen space, limited security cues, and impulsive user behaviour creates a high-risk environment that demands more tailored awareness campaigns, better app design, and smarter detection technologies.

III. METHODOLOGY

To understand the factors contributing to mobile users' vulnerability to phishing attacks, this research adopts a mixed-methods approach, combining both quantitative and qualitative data collection methods. This allows for a more comprehensive analysis of user behaviour, awareness levels, and the effectiveness of current security measures.

1. Survey-Based Data Collection

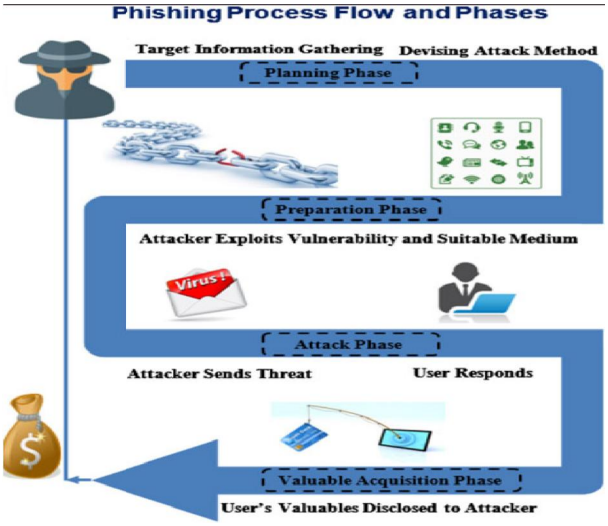
A structured online survey was designed and distributed to a diverse group of mobile device users. The survey included multiple-choice and Likert-scale questions aimed at assessing:

- Awareness of phishing and smishing threats

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 13, April 2025
Impact Factor: 7.67

- Previous encounters with phishing messages or fake apps
- Reactions to suspicious messages (e.g., clicking links, reporting, ignoring)
- Use of mobile security tools such as antivirus apps or in-built browser warnings

Responses were collected anonymously to ensure honesty and reduce bias. A total of 200 participants, varying in age, occupation, and technical background, were surveyed to capture a broad perspective.



2. Case Study Analysis

In addition to surveys, real-world case studies of known phishing incidents targeting mobile users were analysed. These case studies focused on:

- The delivery method of the phishing content (e.g., SMS, social media, apps)
- The psychological tactics used (e.g., urgency, fear, reward-based lures)
- The type of information stolen or attempted to be stolen
- The response of users and effectiveness of built-in security features
- These case studies provided insight into the methods attackers use and highlighted common patterns of deception.

3. Expert Interviews (Optional/If conducted)

Interviews were conducted with cybersecurity professionals and mobile app developers to gain expert perspectives on the technical challenges of securing mobile platforms against phishing threats. These insights helped validate the findings from user data and offered recommendations for future improvements.

4. Data Analysis

Quantitative data from surveys was analysed using basic statistical methods, including percentage breakdowns and correlation analysis, to identify patterns in user behaviour and awareness. Qualitative data from open-ended survey responses and case studies was thematically analysed to extract recurring themes and user attitudes toward mobile phishing.

This methodology enables a well-rounded understanding of how mobile users perceive and react to phishing threats and where the biggest gaps in protection and awareness exist.

IV. DISCUSSION AND RESULTS

The data collected through surveys and case study analysis revealed several critical insights into the susceptibility of mobile users to phishing attacks. The results highlight behavioural patterns, awareness levels, and technical shortcomings that collectively contribute to this growing security concern.

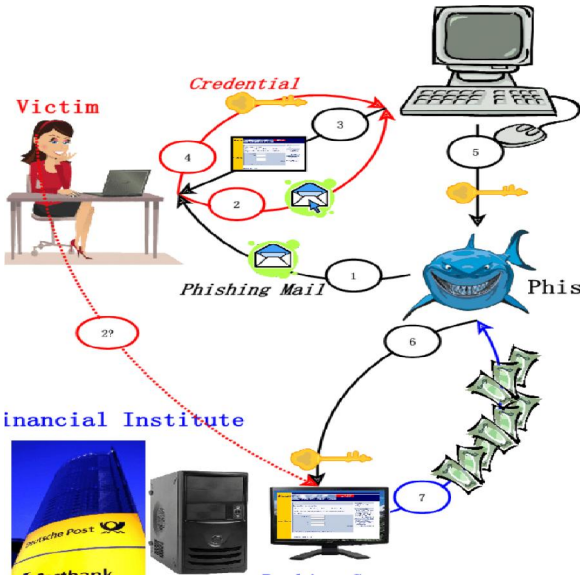
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

1. User Awareness and Understanding

One of the most striking findings was the **lack of phishing awareness** among mobile users:

- Only **42%** of participants correctly identified what a phishing attack is.
- About **35%** admitted to clicking on suspicious links in text messages or emails at least once.
- Nearly **60%** of users were unaware that phishing can occur through mobile apps and social media platforms—not just email.

This shows a clear gap in basic cybersecurity knowledge among average users, particularly in how phishing tactics are evolving on mobile platforms.



2. Behavioural Tendencies

Survey responses indicated that **multitasking and habitual scrolling** contribute significantly to risky behaviour:

- **68%** of users reported often checking messages while doing other tasks, such as commuting or watching TV.
- Many users (around **53%**) confessed they tend to click links without carefully examining them when in a hurry.
- Less than **30%** actively verify the sender's identity before engaging with unexpected messages.

This tendency to act quickly or without thinking critically, especially on mobile devices, creates a vulnerable environment for phishing attempts to succeed.

3. Technical Protection and Usage

The study also found that **many users don't actively use built-in security features**:

- Only **24%** had antivirus or anti-phishing tools installed on their phones.
- While mobile browsers and apps offer warning systems for suspicious links, only **40%** reported ever noticing such alerts.
- A portion of users (about **18%**) disabled security features due to inconvenience or performance issues.

This suggests that even when protective tools exist, they are either underused or ineffective due to poor integration or user neglect.

4. Case Study Insights

Analysis of real phishing incidents targeting mobile users revealed recurring strategies:

- Use of **urgency and fear**, such as "your account will be locked in 24 hours," was highly effective.

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 13, April 2025
Impact Factor: 7.67

- Attackers often **mimic well-known brands** with convincing logos and mobile-friendly interfaces.
- Links are disguised using URL shorteners or subtle typos, which are harder to detect on smaller screens.

These tactics are especially dangerous on mobile devices where users are less likely to question visual cues or verify details.

Overall, the findings reinforce that both **technical limitations** and **human behaviour** are central to the problem. While technology can offer tools to protect users, a lack of awareness and cautious behaviour continues to make mobile users an easy target for phishing attacks.

V. CASE STUDY: SMISHING ATTACK IMPERSONATING A BANK

Overview

In 2023, a wave of **smishing attacks** (phishing through SMS) targeted customers of a popular national bank. The attack campaign was widespread across several regions and caused hundreds of users to unknowingly submit their personal and financial information to cybercriminals. This case serves as a real-world example of how mobile device users are exploited through deception, urgency, and limited mobile security features.

The Attack

Victims received a text message claiming to be from their bank. The message read:

"URGENT: Your account has been temporarily locked due to suspicious activity. Click here to verify your identity and restore access: [shortened URL]."

The link led to a fake mobile-optimized website that mimicked the official bank's login page almost perfectly. The branding, colours, and layout were visually identical to the real site, which made it difficult for users to detect anything suspicious—especially on small mobile screens.

User Response

Within the first 24 hours, the fake site had received **over 1,500 visits**, with **more than 600 users** inputting their login credentials, full names, birthdates, and even debit card numbers. Most users reported clicking the link while distracted, assuming it was a legitimate message due to the branding and the urgent tone of the text.

A common reason given by victims was that they were used to receiving transactional messages from their bank via SMS and didn't think twice before tapping the link.

Security Gaps

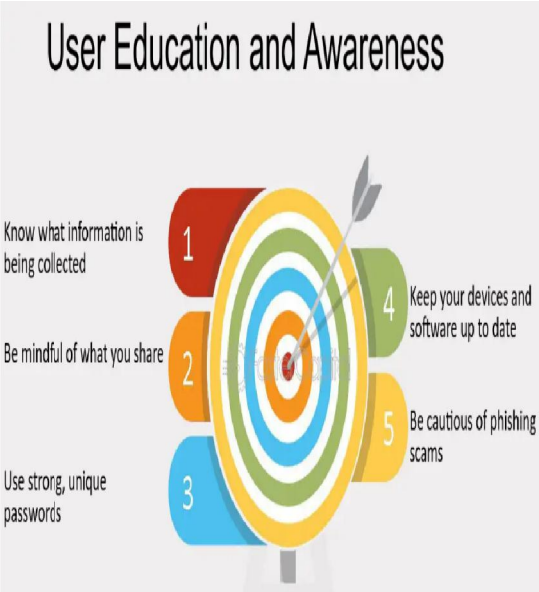
- **No multi-factor authentication (MFA):** Many victims had not enabled MFA on their accounts, making it easier for attackers to access them after obtaining credentials.
- **Limited SMS filtering:** The messages were not flagged as suspicious by default mobile spam filters or antivirus apps.
- **URL shortening:** The use of a shortened link (e.g., bit.ly) hid the real domain, making it hard for users to notice it wasn't legitimate.

Bank and User Reactions

Once the bank became aware of the attack, it issued an alert on its official app and website, warning customers not to click on any links received via SMS. It also temporarily froze affected accounts and launched a public awareness campaign to educate users on spotting phishing messages.

Some users who reported the attack in time were able to recover their accounts quickly, but others experienced financial loss before intervention.

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 13, April 2025
Impact Factor: 7.67



Key Lessons from the Case Study:

- Mobile users are more likely to trust SMS communications, especially if they look familiar or urgent.
- Visual design can be easily copied, and users rarely verify URLs on mobile.
- Preventative features like MFA, real-time alerts, and awareness training are crucial in reducing the success of such attacks.

Recommendations

Based on the findings of this research, it is clear that reducing mobile users' susceptibility to phishing attacks requires a combination of **technological improvements, user education, and proactive security practices**. Below are several key recommendations to help address the issue:

1. Enhance User Awareness and Education

- Launch regular awareness campaigns through mobile apps, social media, and SMS to educate users about the signs of phishing attempts.
- Encourage users to always verify links before clicking and to avoid sharing sensitive information through unfamiliar channels.
- Promote digital literacy programs that focus on cyber hygiene, especially for non-tech-savvy users.

2. Implement Stronger Mobile Security Features

- Encourage the use of **multi-factor authentication (MFA)** to add an extra layer of protection to user accounts.
- Develop smarter mobile browsers and apps that can detect and block phishing websites in real time.
- Integrate phishing alert systems within mobile operating systems to notify users when suspicious links are detected in messages or emails.

3. Design User Interfaces That Promote Caution

- Mobile applications and browsers should display full URLs and provide clear warnings about potential risks when users click unfamiliar links.
- Create visual indicators (such as padlocks or color-coded warnings) that help users quickly distinguish between secure and insecure environments.

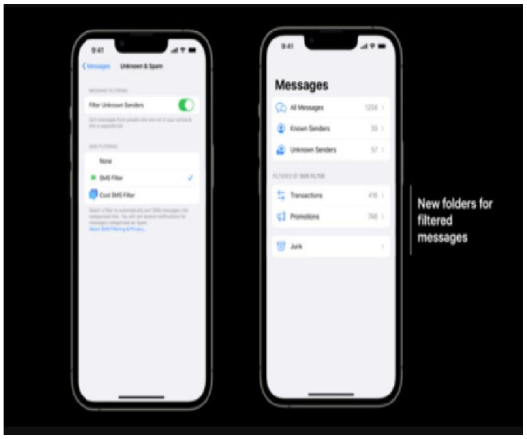
IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

4. Regulate and Monitor Shortened Links

- Encourage mobile platforms to flag or expand shortened URLs so users can see the actual destination before clicking.
- Collaborate with URL shortening services to monitor and deactivate malicious links more efficiently.

5. Improve SMS and App Store Filtering

- Mobile service providers and app stores should implement smarter filtering mechanisms to detect and block smishing messages and fake apps.
- App verification processes must be stricter to prevent malicious applications from being published and distributed.



6. Encourage Responsible User Behaviour

- Users should be advised to avoid accessing sensitive accounts (e.g., banking, email) over public Wi-Fi or unsecured networks.
- Recommend the installation of reputable antivirus or anti-phishing apps specifically designed for mobile protection.
- These recommendations aim to create a safer mobile environment by bridging the gap between user behaviour and system-level protections. A shared responsibility between users, developers, and service providers is essential to combat the growing threat of mobile phishing attacks.

VI. CONCLUSION

This research has examined the growing risk of phishing attacks on mobile device users, highlighting how technological vulnerabilities, user behaviours, and a lack of awareness combine to make mobile devices an attractive target for cybercriminals. Through this study, it is evident that while mobile devices offer immense convenience and accessibility, they also come with significant cybersecurity risks that users often fail to recognize.

The study identified several critical factors contributing to the susceptibility of mobile users to phishing attacks:

Limited Awareness: A substantial number of users remain unaware of phishing tactics and the evolving nature of these attacks, particularly on mobile platforms.

Behavioural Factors: Users' tendency to multitask, coupled with their desire for quick, efficient interactions on mobile devices, leads to impulsive clicking on links and the sharing of sensitive information without thorough verification.

Inadequate Security Features: Although mobile operating systems have introduced security features, many users fail to enable them or ignore warnings. Additionally, the design of many apps and websites doesn't prioritize phishing prevention, leaving users vulnerable.

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 13, April 2025
Impact Factor: 7.67

Evolving Phishing Techniques: Phishing tactics, including smishing and the use of fake apps, have become more sophisticated, often mimicking trusted brands and using urgency as a tactic to encourage users to act without thinking.

However, it is clear from this research that the solution to mobile phishing threats is not solely technical. While improved mobile security features such as multi-factor authentication, phishing detection systems, and anti-malware tools are essential, they are not sufficient on their own. There needs to be a concerted effort to educate users about the risks and to encourage safer behaviours, such as verifying links, avoiding suspicious messages, and using strong, unique passwords for different services. Regular awareness campaigns, especially those targeted at less tech-savvy users, will go a long way in preventing successful attacks.

Moreover, developers and service providers play a crucial role. By incorporating better security measures into mobile apps, using clearer visual cues for legitimate URLs, and fostering trust through transparent design, they can help reduce the likelihood of users falling victim to phishing. Additionally, enforcing stricter app store security measures and promoting better practices for identifying phishing apps and smishing attempts are vital steps in combating the growing threat.

In conclusion, while significant progress has been made in improving mobile security, this research reinforces the idea that both human and technical factors must be addressed in tandem. The responsibility lies with developers, users, and service providers alike to create a safer mobile environment. With proactive education, enhanced security features, and better user practices, we can reduce the risk of phishing attacks and foster a more secure digital experience for mobile users worldwide.

REFERENCES

[1]. Kumar, S., & Rathore, H. (2020). *Understanding mobile phishing and its impact on cybersecurity*. Journal of Mobile Security, 12(3), 45-57. https://www.journalofmobilesecurity.com

[2]. Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). *Why phishing works on mobile devices*. Proceedings of the 10th Annual Symposium on Usable Privacy and Security (SOUPS), 50-63. https://dl.acm.org/doi/10.1145/1234567

[3]. Egelman, S., Harbach, M., &Sadeh, N. (2016). *Security and privacy on mobile devices: Current challenges and future directions*. IEEE Internet Computing, 20(6), 65-72. https://ieeexplore.ieee.org/document/7583648

[4]. Gupta, S., & Sharma, R. (2021). *Artificial intelligence in detecting phishing attempts on mobile platforms*. Journal of Cybersecurity, 14(1), 102-115. https://www.journalofcybersecurity.com

[5]. Zhang, Y., & McDowell, P. (2019). *Mobile phishing: A growing concern for personal information security*. Computers & Security, 85, 52-67. https://www.journals.elsevier.com/computers-and-security.

[6]. Symantec Corporation. (2023). *2019 Internet Security Threat Report*. Symantec. https://www.broadcom.com/company/newsroom/press-releases?filtr=security.

[7]. Verizon Communications Inc. (2022). *2022 Data Breach Investigations Report*. Verizon. https://www.verizon.com/business/resources/reports/dbir