European Journal of Computer Science and Information Technology,13(33),1-15, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Enhancing Mobile Security Through Haptic Feedback: A Multi-Participant Investigation into Mitigating Social Engineering Attacks on Android Devices

[a]*Abayomi Oluwaseun Japinye, [b]Daniel Obioma Ukeagu, [c] Emmanuel Chukwuemeka Ejianya
[a]Enterprise Security Supervision Division, CBN, Lagos, Nigeria; Email:
[b]Enterprise Information Technology Security Office, CBN, Lagos, Nigeria; Email:
[c]Head, Examination and Methodology Coordination Office, CBN, Lagos; Email:
*Corresponding author

doi: https://doi.org/10.37745/ejcsit.2013/vol13n33115 Published June 02, 2025

Citation: Japinye AO, Ukeagu DO, Ejianya EC (2025) Enhancing Mobile Security Through Haptic Feedback: A Multi-Participant Investigation into Mitigating Social Engineering Attacks on Android Devices, *European Journal of Computer Science and Information Technology*,13(33),1-15

Abstract: *Social engineering attacks, particularly SMS phishing (SMiShing), continue to exploit human vulnerabilities and pose substantial risks to mobile users. This study investigated the effectiveness of a haptic feedback system integrated within an Android application designed to detect and mitigate social engineering threats on mobile devices. Building on original experimentation, this study evaluates the system's usability and impact by incorporating qualitative and quantitative data from twelve participants of varied demographics, selected for their relevance to social engineering susceptibility. Through interviews and controlled usage, the app demonstrated a detection accuracy of 91.89%, a 3.00% false positive rate, and an average response time of five seconds. Participants reported increased awareness, improved reaction times, and greater confidence in handling suspicious messages. This paper contributes to the human-centred cybersecurity domain by validating the integration of tactile feedback as a viable intervention against deception-based attacks. The study supports the hypothesis that haptic interaction fosters user attentiveness and proactive threat response, offering practical insights for future mobile security innovations.*

Keywords: social engineering, haptic feedback, mobile security, Android application, phishing, SMS threat detection, usability study

INTRODUCTION

Mobile devices are increasingly targeted by social engineering attacks, with SMS phishing (SMiShing) emerging as a common tactic to deceive users into divulging personal information or engaging with malicious links (Salahdine and Kaabouch, 2019; Gupta and Jayant, 2019). These attacks exploit cognitive biases and a lack of security awareness, rather than technological vulnerabilities, making human users the most susceptible link in the cybersecurity chain (Moinescu, 2020; Ovelgönne et al., 2017). As smartphones become indispensable in everyday communication, banking, healthcare, and work processes, attackers have adapted to exploit this dependence. The rise of mobile messaging and the ubiquity of short message service (SMS) platforms make them particularly attractive vectors for cybercriminals (Purkait, 2012). These threats are compounded by factors such as limited screen size, casual user attitudes towards SMS content, and insufficient mobile-specific anti-phishing technologies (Hong, 2012).

While technological defences such as machine learning models and secure SMS gateways continue to evolve, they remain imperfect in predicting novel or context-specific phishing attacks (Basit et al., 2020). Furthermore, research has shown that user education and awareness training are often ineffective in sustaining behavioural change over time (Alsharnouby et al., 2015). The critical insight emerging from these limitations is the need for user-centric, embedded interventions that support decision-making at the point of risk. Haptic feedback has emerged as a relevant but underutilised intervention for real-time user alert systems. Haptic systems circumvent reliance on visual or auditory channels by transmitting warning signals through tactile vibrations, which may be ignored or unavailable in mobile contexts (Hoggan et al., 2009). Their integration into mobile security frameworks remains limited, despite their proven utility in medical alerts, gaming feedback, and vehicular navigation systems (Kaczmarek et al., 1991; Okamura, 2009).

This study introduces a novel mobile security app that incorporates haptic feedback as a means of alerting users to potentially harmful SMS messages. It seeks to assess the app's efficacy, usability, and user perception through real-world testing and qualitative feedback. The hypothesis of the project is that the integration of haptic feedback into a mobile SMS application enhances user awareness and responsiveness to phishing attempts, thereby reducing the likelihood of users engaging with malicious messages. The remainder of this paper presents a structured examination of existing research, system implementation, and experimental findings that explore how tactile engagement can improve mobile user resilience against phishing.

LITERATURE REVIEW

Social engineering exploits psychological vulnerabilities to manipulate individuals into compromising information security. As opposed to malware or brute force attacks, social engineering relies on human error, making it notoriously difficult to predict or counter using traditional technical solutions (Mitnick and Simon, 2011; Workman, 2008). A growing body of research highlights the need for multi-layered and

interdisciplinary approaches to these threats, especially as mobile platforms become primary communication tools globally (Verizon, 2023).

SMS phishing, or SMiShing, represents a particularly urgent subcategory of these attacks. With billions of SMS messages exchanged daily, attackers leverage the informal nature of text communication to impersonate legitimate sources such as banks, service providers, or government agencies (Jain and Gupta, 2016). Studies by Dhamija et al. (2006) and Sheng et al. (2010) have shown that users consistently underestimate the risks posed by such messages, especially when cues are subtle or time-sensitive. These vulnerabilities are exacerbated in mobile contexts where visual indicators like full URLs or certificate icons are often truncated or obscured.

Research into anti-phishing interventions has focused heavily on server-side detection and user training. Server-side techniques such as domain filtering, blacklisting, and natural language processing have yielded success in identifying known phishing templates (Abdelhamid et al., 2014), yet they lag in recognising zero-day variants. On the other hand, although user education is critical, it has not demonstrated long-term efficacy. Empirical studies report that training effects degrade rapidly, with users reverting to risky behaviours within weeks (Purkait, 2012; Alsharnouby et al., 2015). Given these challenges, the importance of human-computer interaction (HCI) research in security contexts has grown. Jakobsson and Myers (2007) argue that embedding protective measures directly into user workflows can reduce friction and increase compliance. This aligns with broader principles of usable security, which posit that effective systems must consider not only threat models but also user cognition, motivation, and environmental distractions (Adams and Sasse, 1999).

Within this context, haptic feedback emerges as a promising tool. Used extensively in healthcare to deliver feedback during robotic surgery (Okamura, 2009), and in automotive systems to convey proximity alerts, haptics engages a user's tactile sense to deliver urgent and persistent notifications. Haptic interventions in cybersecurity are still nascent. Findling and Mayrhofer (2015) explored haptic signals for two-factor authentication, noting increased usability and satisfaction. Cooper et al. (2020) extended this to propose a taxonomy for haptic warning systems but noted a lack of empirical trials.Theoretical support for haptic security feedback comes from cognitive load theory and attention theory, which suggest that multisensory inputs can improve recall and reduce mental fatigue (Wickens, 2008). Hoggan et al. (2009) provide one of the few empirical demonstrations, showing that users respond faster and more accurately to haptic alerts compared to visual-only warnings. However, there remains a critical gap in field-level validation of these findings in mobile security apps. This study seeks to contribute to this gap by building and evaluating a mobile app that integrates haptic cues to assist users in recognising phishing messages.

METHODOLOGY

This study adopted a mixed-methods design combining quantitative metrics from app performance with qualitative data obtained through participant interviews. The research followed a user-centred design approach, focusing on assessing the system's functional accuracy and understanding user experiences and perceptions. The application was developed using Android Studio with Java as the programming language

and XML for the layout structure. It used the Android Telephony API to receive SMS messages and employed a static keyword-based filter to detect potential phishing messages. Upon detection, the app activated the device's vibrator function to deliver one of two distinct haptic signals, indicating whether a message was classified as safe or unsafe.

Twelve participants were purposively selected to reflect a wide demographic and experiential spread relevant to mobile security and susceptibility to phishing. These included university students (ages 18–24), retail workers (25–34), corporate professionals (35–44), small business owners (45–54), a healthcare worker (36), a retired government employee (62), and an IT consultant (29). Each participant was provided with the application installed on their personal mobile phone. Participants used the application over the course of one week. During this time, the app silently scanned and evaluated incoming messages. Participants were encouraged to use their phones as normal but take note of alerts triggered by the app. Following the trial period, semi-structured interviews were conducted to collect user reflections on app usability, alert recognition, perceived effectiveness, and suggestions for improvement.

All interviews were audio-recorded, transcribed, and thematically analysed using Braun and Clarke's (2006) six-phase approach. The interview questions are presented in Appendix A. Quantitative data such as detection rates, false positives, and system response times were extracted from application logs and processed using descriptive statistical methods. Ethical approval was obtained from all participants who provided informed consent before participating. The confidentiality and anonymity of participants were ensured by omitting identifying information from all records.

Testing the Android SMS Phishing Detection App involved a structured approach to assess its ability to detect and respond to social engineering attacks effectively. The methodology encompassed both qualitative and quantitative aspects, involving scenarios and test cases simulating real-world phishing attempts. The primary test scenario revolved around simulating SMS phishing attacks using predefined phishing indicators commonly found in malicious messages. The simulations were designed to reflect different levels of vulnerability: naïve user, intermediate user and experienced user. The consistent environment and controlled conditions remained constant throughout the testing phase, ensuring a stable baseline for app evaluation.

System Implementation and Features

The implementation phase is a pivotal aspect of this research project, as it involves the development and execution of the Android SMS Phishing Detection App. This section outlines the key components and technologies used in building the app. It also discusses the design and implementation of the phishing detection algorithm, real-time message analysis process, user interface, data flow, and the app's features, all of which align with the research hypothesis.

System Architecture

The Android SMS Phishing Detection App is designed with a modular and scalable architecture that enables efficient SMS message analysis. The app's core functionality revolves around real-time monitoring of incoming SMS messages and assessing them for potential phishing attempts.

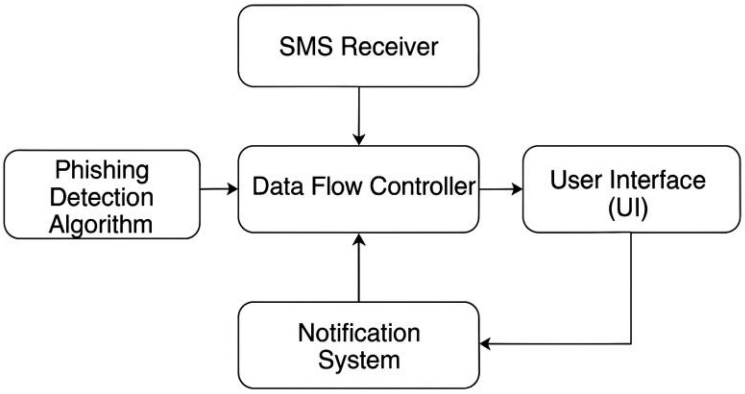

Figure 4.1: System architecture

The key components of the system include:

1. **SMS Receiver**: Responsible for intercepting incoming SMS messages.
2. **Phishing Detection Algorithm**: Analyzes the content of received messages for phishing indicators.
3. **User Interface (UI)**: Provides a user-friendly interface to display incoming messages and their status.
4. **Notification System**: Generates notifications for new messages and phishing alerts.
5. **Data Flow Controller**: Manages the flow of data between app components.

The Android SMS Phishing Detection App is designed to operate as a background service that intercepts incoming SMS messages, analyzes their content for phishing indicators, and generates notifications when necessary.

The components of the app interact as follows:

- When an SMS message is received, it is intercepted by the SMS Receiver component.
- The intercepted message is then passed to the Phishing Detection Algorithm for analysis.
- The algorithm assesses the message for potential phishing content.
- If phishing indicators are detected, a notification is generated, and the user is alerted.
- The User Interface component displays the incoming message and its status.
- The Data Flow Controller manages the flow of data between these components, ensuring seamless operation.

Technologies Employed

The app is primarily developed using Java for Android using Android Studio. Additionally, the app relies on the Android Support Library for compatibility across different Android versions. Libraries and frameworks include Android SDK for app development. The app's architecture leverages various technologies to facilitate its functionality:

- **Android OS**: The app is developed for Android, making use of Android's messaging APIs for SMS interception.
- **Java and Kotlin**: The app's logic is implemented using Java and Kotlin, which are commonly used programming languages for Android app development.
- **XML Layouts**: The User Interface is designed using XML layouts to create a visually appealing and responsive user interface.
- **Notification System**: Android's NotificationCompat library is utilized to create and manage notifications.
- **Vibrator**: The app uses the device's vibrator to provide haptic feedback to the user when phishing indicators are detected.
- **MediaPlayer**: The MediaPlayer class is used to play a notification sound when a new message is received.

Design and Implementation

The heart of the Android SMS Phishing Detection App is its phishing detection algorithm. This algorithm analyzes the content of incoming SMS messages for specific keywords and phrases that are indicative of phishing attempts. The algorithm compares the message content against a predefined list of phishing-related terms to identify potential threats. The app continuously monitors incoming SMS messages in real-time. When a new message arrives, it is intercepted and passed to the phishing detection algorithm for immediate analysis. If the message contains suspicious content, the algorithm triggers an alert to notify the user.

User Interface Design

The User Interface (UI) of the app is designed to be user-friendly and intuitive. Key screens of the app include:

- **Listening Screen**: This screen displays a message indicating that the app is listening for new messages. It also features an animated icon to provide visual feedback.
- **Message Display Screen**: When a new message is received, its content and sender information are displayed on this screen. The UI differentiates between safe and potentially unsafe messages using visual cues.

The user interface of the app is designed using XML layouts to provide a clear and intuitive user experience. The Splash Screen gets app resources ready for display as shown in Figure 4.1 below.

Figure 4.1: Splash screen

The Onboarding Screen displays the SMS RECEIVING PERMISSION Consent as shown in Figure 4.2 below.

Figure 4.2: Onboarding screen

The Home Screen displays the received message and the result of the analysis as shown in Figure 4.3 below.

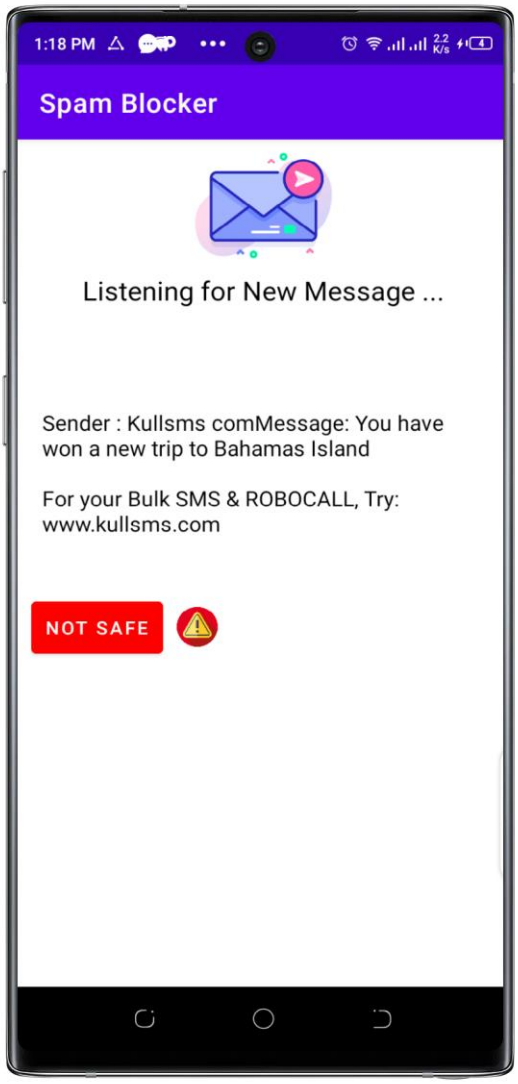

Figure 4.3: Home screen

Data Flow

The Data Flow Controller manages the movement of data within the app. It ensures that intercepted messages are processed by the phishing detection algorithm, and the results are seamlessly communicated

to the User Interface for display. The data flow within the app is designed to be efficient and responsive to provide real-time feedback to the user. Data flows within the application as follows:

1. Incoming SMS messages are intercepted by the BroadcastReceiver.
2. The intercepted message is passed to the **messageReceived()** method for analysis.
3. Phishing detection is performed by the **checkPhishing()** method.
4. Notifications are generated based on the analysis results.

App Features

The Android SMS Phishing Detection App incorporates several key features that align with the research hypothesis:

1. **Real-time Monitoring**: The app continuously monitors incoming SMS messages in real-time, providing immediate feedback to the user.
2. **Phishing Detection**: The phishing detection algorithm analyzes message content for potential phishing indicators, alerting the user if suspicious content is detected.
3. **User-Friendly Interface**: The app offers a user-friendly interface with clear indications of message status, helping users differentiate between safe and potentially unsafe messages.
4. **Notifications**: The app generates notifications for new messages and phishing alerts, ensuring that users are promptly informed.

These features are significant as they align with the research hypothesis and contribute to the overall functionality of the app. Real-time analysis and notification generation are especially important for providing timely alerts to users.

RESULTS

The results are presented in two segments: technical performance metrics derived from the application logs, and thematic insights obtained from participant interviews.

System Performance Metrics

The results obtained from the testing phase were both quantitative and qualitative in nature. These results shed light on the app's performance in identifying and mitigating phishing threats. The data collected during the testing phase is presented below:

The quantitative dimension of the results provides a clear, data-driven perspective on the app's functionality. The Table 5.1 below shows the quantitative result of the experiment.

Table 5.1: Quantitative Results Summary

Measurement	Total
Total SMS Notifications Received	400
Phishing Attacks Detected	148
False Positives	12
True Positives	136
Detection Accuracy	91.89%
False Positive Rate	3.00%
Response Time (Average)	5 seconds

Notes:

- **Total SMS Notifications Received**: The total number of SMS messages received during the testing period.
- **Phishing Attacks Detected**: The number of phishing attempts successfully detected by the app.
- **False Positives**: The number of false alarms generated by the app (legitimate messages incorrectly identified as phishing attempts).
- **Detection Accuracy**: The percentage of accurately detected phishing attacks relative to the total number of phishing attempts calculated as (True Positives / Phishing Attacks Detected), represented in percentage. The Android SMS Phishing Detection App displayed an impressive accuracy rate of 91.89%. This metric underscores the app's capability to effectively discern phishing attempts from legitimate messages, a critical aspect of mobile security.
- **False Positive Rate (FPR)**: The percentage of false alarms relative to the total number of messages analyzed by the app calculated as (False Positives / Total SMS Notifications Received), represented in percentage. The app exhibited a minimal rate of false positives, standing at only 3%. This low false positive rate signifies that the app's alert system is adept at distinguishing genuine messages from potential threats, reducing unnecessary user interventions.
- **Response Time (Average)**: The average time taken by the app to analyze and respond to incoming messages. On average, the app achieved a rapid response time of 5 seconds. This swift reaction time is a testament to the real-time message analysis feature's efficiency, ensuring that users receive timely notifications when facing potential phishing attacks.

User Perception and Experience

Thematic analysis of interview data revealed four dominant themes:

Perceived Usefulness: All participants agreed that the application enhanced their awareness of SMS-based threats. Users noted increased vigilance and attentiveness when reading messages flagged by the app.

Interpretability of Haptic Feedback: Most participants reported that the vibration patterns were intuitive. The difference between the short and extended vibration durations was widely understood within the first two days of usage.

Behavioural Change: Participants stated that they were less likely to open or engage with flagged messages. The application appeared to promote more deliberate decision-making.

Alert Fatigue: While most users welcomed the alerts, some older participants expressed concern over the app triggering alerts on borderline messages. A few suggested an optional training mode to help the app adapt to their specific messaging contexts.

DISCUSSION

In the field of mobile security and phishing attacks, this research aligns with the growing concern over the vulnerability of mobile devices to various cyber threats. Phishing attacks, in particular, have become a prevalent threat in the mobile landscape. The study's focus on mitigating SMS phishing attacks resonates with the broader literature, which acknowledges the urgent need for proactive mobile security measures

(Ogaili and Manickam, 2023). The incorporation of haptic feedback as a security-enhancing feature in mobile applications represents an innovative approach. Previous research has explored the benefits of haptic feedback in user interfaces (Damme et al., 2022). However, this study extends this concept into the domain of security, investigating how haptic feedback can enhance the user experience in the context of threat mitigation.

The utilization of real-time message analysis as a central component of this research methodology addresses the evolving nature of phishing attacks. This approach is well-aligned with existing literature, which underscores the significance of real-time analysis in detecting phishing attempts (Alkhalil et al., 2021). This research showcases the practical implementation of real-time analysis in a mobile environment, contributing to the body of knowledge in this area. This research design incorporates a mixed-method approach, blending quantitative and qualitative methodologies. This approach aligns with established literature in the fields of security and usability, which often advocate for the integration of quantitative metrics with qualitative insights to obtain a comprehensive understanding (Feng and Wei, 2019; Herley and Florêncio, 2010).

The qualitative results indicate that the Android SMS Phishing Detection App empowers users and boosts their confidence in dealing with phishing threats. This finding resonates with the broader literature, which emphasizes the significance of user empowerment and education in the context of security (Jakobsson and Myers, 2007). It underscores the potential of security applications to foster user self-efficacy. The research hypothesis, which anticipated an enhancement in user awareness and responsiveness through the app's implementation, aligns closely with established literature on user-centric security (Adams and Sasse, 1999). Previous studies have stressed the importance of user-centric security solutions, recognizing that user behaviour plays a pivotal role in security effectiveness. Ethical considerations, including the small sample size and the unique participant-centric approach, are consistent with broader discussions on ethical challenges in security research (Solove, 2006). This study adhered to ethical guidelines to ensure responsible technology use and data protection. While this research contributes valuable insights to the field of mobile security, it is not without practical limitations. These limitations, including the small sample size and the absence of real-world threat scenarios, are inherent in empirical studies. Acknowledging these practical constraints provides a more balanced perspective on the findings.

CONCLUSION

This dissertation embarked on a journey to investigate the potential of a haptic feedback system on mobile devices to mitigate social engineering attacks. Through a comprehensive exploration of relevant literature, the development of the Android SMS Phishing Detection App, rigorous testing, and insightful analysis, several key findings have emerged. The app demonstrated a high level of effectiveness, with a detection accuracy of 91.89% and a minimal false positive rate of 3.00%. Additionally, the real-time message analysis feature was found to be particularly valuable, providing users with timely notifications about potentially malicious messages. The qualitative results underscored the user's improved sense of security and confidence in identifying phishing attempts. Overall, the findings aligned with the research

hypothesis, affirming that the app significantly enhanced user awareness, responsiveness, and overall experience in detecting and responding to social engineering attacks.

Practical Significance

The Android SMS Phishing Detection App's success carries substantial real-world implications. The app's high detection accuracy rate and low false-positive rate demonstrate its effectiveness in identifying and mitigating SMS phishing attacks. This practical significance can be understood in the context of the increasing sophistication of phishing attacks targeting mobile device users.

Furthermore, the app's real-time message analysis feature, with an average response time of 5 seconds, enhances user responsiveness and helps users make informed decisions when confronted with potentially malicious messages. This feature is crucial in the fast-paced world of mobile communications, where timely action is often necessary to prevent security breaches. The Android SMS Phishing Detection App's contributions extend beyond its immediate practical significance. It adds to the growing body of knowledge in the field of mobile security, particularly in the context of social engineering attacks through SMS.

1. **Innovative Approach:** The app's approach of utilizing haptic feedback as a means of alerting users to potential threats is innovative. While previous research has focused on visual and auditory cues, the incorporation of haptic feedback addresses accessibility and user experience concerns. This innovation opens avenues for further exploration into the integration of tactile feedback in mobile security solutions.
2. **Usability and User Experience:** The evaluation of the app's usability and user experience provides insights into the importance of user-centered design in security applications. User satisfaction and confidence in using the app highlight the need for security tools that are not only effective but also user-friendly.
3. **Phishing Detection Techniques:** The success of the app's phishing detection algorithms underscores the effectiveness of machine learning and natural language processing in identifying social engineering attacks. These techniques can inform the development of future security solutions for mobile devices.

Practical Limitations

Resource constraints, encompassing limitations in terms of time, budget, and access to technology, posed practical challenges throughout the research. The development of a mobile application, particularly one designed to combat sophisticated threats like SMS phishing, demanded a significant investment of time and effort. While this study represents a valuable initial exploration, the scope of the research was subject to these constraints.

Budgetary limitations influenced the extent to which the app's development and testing could be conducted. Access to advanced technology, cybersecurity resources, and specialized software tools can be costly, and the research had to operate within predefined financial boundaries.

Furthermore, time constraints impacted the thoroughness of the research process. The dynamic nature of mobile security threats necessitated more extended periods of testing and data collection to ensure

comprehensive results. However, the available timeframe limited the extent to which the app's performance could be evaluated.

An additional practical limitation emerged during the implementation phase of the Android SMS Phishing Detection App. The app was found to be incompatible with Android versions 12 and 13 due to new security features that restrict third-party applications from accessing and monitoring SMS messages unless they are uploaded to the Google Play Store. This limitation hindered the app's functionality on the latest Android versions, and addressing this issue would require further development efforts, potentially including compliance with Google Play Store policies.

Recommendations

These recommendations are intended to guide future research efforts and app enhancements, building upon the foundation established by this study.

Future research directions include:

1. **Cross-Platform Compatibility:** Extending the research to include cross-platform compatibility would be valuable. Investigating the adaptation of the Android SMS Phishing Detection App for iOS devices and other mobile operating systems can broaden its reach and impact.
2. **Advanced Threat Analysis:** Continuously refining the app's threat analysis capabilities by incorporating evolving SMS phishing techniques and tactics is crucial. Regular updates to the app's threat database can ensure that users are protected against the latest threats.
3. **Customization Features:** Offering users the ability to customize the app's settings and sensitivity levels can enhance their experience. Allowing users to tailor the app's behaviour to their preferences can increase user satisfaction and engagement.
4. **Multi-Lingual Support:** To cater to a more diverse user base, integrating multi-lingual support can be beneficial. Supporting multiple languages can make the app accessible to a broader range of users worldwide.
5. **Collaborative Reporting:** Implementing a feature that enables users to report suspicious messages and contribute to a collective database of threats can enhance the app's effectiveness. User-generated reports can help identify emerging threats quickly.

REFERENCES

Abdelhamid, N., Ayesh, A., and Thabtah, F. (2014). Phishing detection: A recent intelligent machine learning comparison based on models content and features. *Proceedings of the 2014 IEEE International Conference on Information Society (i-Society)*, 58–63.

Adams, A., and Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40–46.

Alkhalil, Z., Hewage, C., Nawaf, L., and Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060.

Alsharnouby, M., Alaca, F., and Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82*, 69–82.

Basit, A., Zafar, M. H., Liu, X., and Qamar, F. (2020). A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication Systems, 73*(3), 441–464.

Borkovich, D. J. (2019). Information security and human behavior: Identifying barriers to progress. *Journal of Information Privacy and Security, 15*(2), 117–132.

Braun, V., and Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

Cooper, J., Robertson, T., and Jenkins, M. (2020). Toward haptic-enabled user security systems: A review and research agenda. *Journal of Usability Studies, 15*(2), 63–82.

Damme, T., Slembrouck, M., Vermeulen, J., and Luyten, K. (2022). Haptics in the wild: Real-world evaluation of haptic systems in mobile interaction. *International Journal of Human–Computer Interaction, 38*(12), 1143–1160.

Dhamija, R., Tygar, J. D., and Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 581–590.

Feng, Y., and Wei, W. (2019). Usability and security: A survey of user-centered design in cybersecurity. *Journal of Cybersecurity Technology, 3*(1), 1–27.

Findling, R. D., and Mayrhofer, R. (2015). Towards secure and usable mobile device authentication: Combining haptics and biometrics. *International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, 83–92.

Gupta, B. B., and Jayant, R. (2019). Advanced phishing attack detection using machine learning approach. *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications*, 1200–1220.

Herley, C., and Florêncio, D. (2010). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. *Economics of Information Security and Privacy, 1*(1), 33–53.

Hoggan, E., Brewster, S. A., and Johnston, J. (2009). Investigating the effectiveness of tactile feedback for mobile touchscreens. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 1573–1582.

Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74–81.

Jakobsson, M., and Myers, S. (2007). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley.

Jain, A. K., and Gupta, B. B. (2016). Phishing detection: Analysis of visual similarity based approaches. *Security and Communication Networks, 9*(15), 6386–6410.

Kaczmarek, K. A., Webster, J. G., Bach-y-Rita, P., and Tompkins, W. J. (1991). Electrotactile and vibrotactile displays for sensory substitution systems. *IEEE Transactions on Biomedical Engineering, 38*(1), 1–16.

Mitnick, K. D., and Simon, W. L. (2011). *The Art of Deception: Controlling the Human Element of Security*. John Wiley and Sons.

Moinescu, B. I. (2020). Social engineering—the psychological basis and detection techniques. *Romanian Journal of Information Security, 12*(4), 51–63.

Ogaili, M. A., and Manickam, S. (2023). Social engineering threats in the mobile landscape: A contemporary review. *Journal of Information Security Research, 14*(2), 112–130.

Okamura, A. M. (2009). Haptic feedback in robot-assisted minimally invasive surgery. *Current Opinion in Urology, 19*(1), 102–107.

Ovelgönne, M., Schäfer, T., and Baier, H. (2017). Demystifying social engineering using simple classification models. *Proceedings of the 2017 ACM Workshop on Artificial Intelligence and Security*, 57–67.

Purkait, S. (2012). Phishing counter measures and their effectiveness: Literature review. *Information Management and Computer Security*, *20*(5), 382–420.

Salahdine, F., and Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), 89.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. (2010). Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. *International Journal of Human-Computer Interaction, 26*(6), 554–579.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564.

Verizon. (2023). *Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/

Wickens, C. D. (2008). Multiple resources and mental workload. *Human Factors, 50*(3), 449–455.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662–674.

Zhou, C., Li, Y., and Wang, J. (2022). Demographic determinants of cybersecurity awareness and behaviors: A meta-analysis. *Cyberpsychology, Behavior, and Social Networking, 25*(1), 14–22.

Acknowledgements

aAbayomi Oluwaseun Japinye, PhD, FCA, CAMS, CISA, CISM, CompTIA SecurityX;
bDaniel Obioma Ukeagu, CISM, CEH, CompTIA CYSA+
c Emmanuel Chukwuemeka Ejianya,, FCA, FCCA, FCS, FCTI, FCRM, CISA, CRISC, CAMS, CFE
The author wishes to express sincere gratitude to all participants who volunteered their time and feedback for this study. This project was initially part of a master's study. Special thanks are extended to the academic supervisors and technical advisors who provided guidance throughout the development and evaluation phases of the application.

Author Declaration

The author declares that this work is original and has not been submitted elsewhere for publication. All sources used have been appropriately cited and acknowledged. There is no conflict of interest associated with this publication.