Ngr. J. Multi. vol-2, issue-8 (Aug-2026) pp-445-453

ISSN: 3108-2750 (E), 3139-8065 (P)

Nexus Global Research Journal of Multidisciplinary

Journal Homepage: https://nexusglobalresearch.com/journal/ngrjm/

Research Article

Development of a Cybersecurity Framework in Mitigating Android Malware and Masquerade Attacks on Aviation Training Devices

Wens Zaren P. Duron [1*], Rina V. Cabansag[2]

[1] *Master in Information Technology, Major in Cyber Security, University of Luzon Graduate School, Dagupan City, Pangasinan, Philippines*

ABSTRACT:

This study developed a context-specific cybersecurity framework for mitigating Android malware and masquerade attacks on aviation training devices. It assessed the level of awareness of aviation training device users regarding Android malware, masquerade attacks, and public education and interventions, and determined users' perceptions of permission-based and anomaly-based detection approaches. The study employed a descriptive survey design coupled with applied research. Fifty-one qualified Android users from the Maintenance Training Program and On-the-Job Training of an aviation training organization participated in the study. A structured questionnaire was administered through Google Forms and formally reviewed by seven experts in Information Technology and Cybersecurity for face and content validity. Descriptive statistics, including frequency, percentage, weighted mean, and ranking, were used to analyze the responses. The results showed that respondents were moderately aware of Android malware (overall mean = 2.92) and masquerade attacks (overall mean = 2.74). Awareness of public education and interventions was also moderate (mean = 3.39), although respondents showed a strong willingness to engage in cybersecurity practices when better informed (mean = 4.10). Perceptions of permission-based detection were favorable (mean = 3.41), while anomaly-based detection received a stronger favorable rating (mean = 3.82). The findings indicate that users recognized the risks associated with mobile threats but had gaps in threat recognition, confidence, and preparedness. Based on the empirical findings and reviewed literature, the researcher developed the MAPER Framework—Monitor, Assess, Prevent, Educate, and Respond. The framework integrates technical safeguards, risk assessment, preventive controls, cybersecurity education, and incident response into a practical mitigation approach for Android devices used in aviation training.

Keywords: Android Malware; Masquerade Attacks; Cybersecurity Awareness; Permission-Based Detection; Anomaly-Based Detection; Aviation Training; MAPER Framework

Citation: Duron, W. Z. P., & Cabansag, R. V. (2026). Development of a cybersecurity framework in mitigating Android malware and masquerade attacks on aviation training devices. Nexus Global Research Journal of Multidisciplinary, 2(8), 445–453.

1. INTRODUCTION:

The increasing use of smartphones and tablets has changed how people communicate, learn, work, and access digital information. Mobile devices are now used not only for personal activities but also for education, training, communication, and access to technical resources. This increased dependence creates a corresponding need to address mobile cybersecurity risks, particularly Android malware and attacks that disguise malicious applications as legitimate software.

Android malware may compromise device security, expose sensitive information, intercept communications, or perform unauthorized activities. Masquerade attacks are particularly difficult to recognize because malicious applications can imitate legitimate applications through familiar names, icons, interfaces, developer information, ratings, or apparent functionality. Users may therefore trust an application based on its appearance or visible indicators before recognizing that it is malicious.

The issue becomes more significant in aviation training environments where mobile devices may serve as convenient learning and reference platforms. Trainees may use Android smartphones to access digital learning resources, technical manuals, training schedules, aviation-related

***Corresponding Author:** Wens Zaren P. Duron, Email: rvcabansag14@gmail.com

Received: 03 Aug 2026 | **Accepted:** 16 Aug 2026 | **Published:** 20 Aug 2026

applications, and communication platforms. Devices may also contain notes, photographs, downloaded training files, credentials, and other information connected with training activities. A compromised device can therefore affect both personal information and training-related resources.

Within the aviation training organization considered in this study, Android devices are used by Maintenance Training Program and On-the-Job Training participants. Because aviation training emphasizes safety, compliance, accuracy, and disciplined procedures, cybersecurity awareness is an important part of responsible technology use. A user who cannot recognize suspicious applications or unusual device behavior may unintentionally expose information or allow malicious software to enter the training environment.

Previous literature cited in the capstone supports a layered approach to mobile security. Research has emphasized application permissions, behavioral monitoring, trusted application sources, regular software updates, organizational policies, and continuous cybersecurity education. Permission-based detection can identify applications that request excessive or unnecessary access, while anomaly-based detection can identify unusual application or device behavior. These approaches are complementary rather than mutually exclusive.

Although many studies have examined Android malware, mobile security awareness, permission analysis, and anomaly detection, the capstone identified limited direct attention to integrating these measures into a mitigation framework specifically for Android devices used by trainees in an aviation training organization. This contextual gap motivated the present study.

The study aimed to develop a cybersecurity framework for mitigating Android malware and masquerade attacks on aviation training devices. Specifically, it sought to determine the users' awareness of Android malware, masquerade attacks, and public education/interventions; determine their perceptions of permission-based and anomaly-based detection; and use the findings as a basis for developing a practical mitigation framework.

2. REVIEW OF RELATED LITERATURE:

Android malware remains a significant mobile security concern because malicious software can exploit device vulnerabilities and user trust. Masquerade attacks are a form of deception in which malicious applications imitate legitimate applications. The literature reviewed in the capstone indicates that attackers may exploit application names, visual design, developer identity, reviews, download counts, and other visible indicators to persuade users to install malicious software.

Application permissions are an important security consideration. Malicious applications may request excessive or unnecessary permissions to obtain access to sensitive device resources. Permission analysis therefore provides a practical mechanism for identifying potentially suspicious applications. However, technical permission analysis is strengthened when users understand why permissions matter and are willing to review them before installation.

Anomaly-based detection provides another layer of protection. Instead of depending only on known malware signatures, anomaly-based approaches examine unusual application, network, or device behavior. The literature cited in the study supports behavioral monitoring as a complementary defense, especially when malicious activity is not easily recognized through conventional indicators.

Cybersecurity education is equally important because human behavior can contribute to successful attacks. Awareness programs, practical demonstrations, simulations, case-based learning, and continuous security reminders can help users recognize suspicious applications, understand permissions, and respond appropriately. The capstone findings similarly indicate that users are more willing to engage in safer practices when they receive appropriate information and education.

Taken together, the literature supports a layered cybersecurity strategy combining monitoring, assessment, prevention, education, and response. The present study translated these principles into the researcher-developed MAPER Framework and applied them to the specific context of aviation training devices.

3. METHODOLOGY:

The study employed a descriptive survey research design coupled with applied research. The descriptive component was used to determine existing levels of awareness and perceptions without manipulating the respondents or study conditions. The applied research component was used to translate the empirical findings and reviewed literature into a practical cybersecurity mitigation framework.

The participants were 51 qualified Android users from the Maintenance Training Program and On-the-Job Training within the aviation training organization. All qualified and available Android users within the identified population were included. Users of other mobile operating systems were excluded because the study specifically focused on Android malware and masquerade attacks.

A structured questionnaire served as the primary research instrument. It covered five areas: Android malware awareness, masquerade attack awareness, public education and interventions, permission-based detection, and anomaly-based detection. The questionnaire used a five-point Likert scale. The instrument was administered through Google Forms.

Before administration, the questionnaire underwent formal review by seven expert reviewers with relevant expertise in Information Technology and Cybersecurity. The review addressed face validity, content validity, clarity, organization, relevance, completeness, and alignment with the study variables. The instrument was revised based on the consolidated recommendations of the reviewers. The capstone did not document a numerical reliability coefficient; therefore, no coefficient was added to the present manuscript.

Data were collected after the necessary permission was secured. Respondents were informed about the study purpose, voluntary participation, information requested, and measures used to protect their responses. The study did not require passwords, PINs, authentication codes, private messages, personal files, photographs, contacts, or application contents, and no software was installed on respondents' devices.

Frequency and percentage were used where appropriate. Weighted means were used to determine the overall level of awareness and perception for each indicator, while ranking identified the highest- and lowest-rated indicators. For awareness, 4.21–5.00 was interpreted as Extremely Aware, 3.41–4.20 as Highly Aware, 2.61–3.40 as Moderately Aware, 1.81–2.60 as Somewhat Aware, and 1.00–1.80 as Not Aware. For perception, the corresponding descriptive equivalents were Strongly Agree, Agree, Neutral, Disagree, and Strongly Disagree.

4. RESULTS AND DISCUSSION:

4.1 Awareness of Android Malware:

The respondents' overall awareness of Android malware was 2.92, interpreted as Moderately Aware. The highest-rated indicator concerned awareness of the possible consequences of malware infection, such as data theft, financial loss, or system damage (mean = 3.50). Regular updating of antivirus or anti-malware software received a mean of 3.10, while familiarity with the term malware received 2.80. The lowest-rated indicator was confidence in recognizing potential signs of malware infection (mean = 2.20). This pattern suggests that respondents understood that malware can cause harm but were less confident in identifying an actual infection. The finding supports the capstone literature emphasizing the importance of examining application permissions and device behavior and reinforces the need for practical cybersecurity education.

Indicator	Mean	Descriptive Equivalent	Rank
Familiarity with the term malware	2.80	Moderately Aware	4
Confidence in recognizing signs of malware infection	2.20	Somewhat Aware	5

Regular updating of antivirus/anti-malware software	3.10	Moderately Aware	2
Awareness of consequences of malware infection	3.50	Highly Aware	1
Experience with malware infection	3.00	Moderately Aware	3
Overall Mean	2.92	Moderately Aware	—

4.2 Awareness of Masquerade Attacks:

Awareness of masquerade attacks obtained an overall mean of 2.74, interpreted as Moderately Aware. The respondents were highly aware of the risks posed by masquerade attacks to personal or organizational digital assets (mean = 3.50), and they reported a moderate level of encounter with examples such as phishing emails and spoofed websites (mean = 3.10). However, familiarity with the concept and confidence in understanding attacker techniques both received 2.30, while preparedness to identify and mitigate threats received 2.50. The results show a clear distinction between recognizing that deceptive attacks are risky and having the knowledge and confidence needed to identify and respond to them.

Indicator	Mean	Descriptive Equivalent	Rank
Familiarity with the concept of masquerade attacks	2.30	Somewhat Aware	4
Concern about risks posed by masquerade attacks	3.50	Highly Aware	1
Encounter with masquerade attacks	3.10	Moderately Aware	2
Confidence in understanding attack techniques	2.30	Somewhat Aware	5
Preparedness to identify and mitigate threats	2.50	Somewhat Aware	3
Overall Mean	2.74	Moderately Aware	—

4.3 Public Education and Interventions

Awareness of public education and interventions obtained an overall mean of 3.39, interpreted as Moderately Aware. The strongest result was the likelihood of engaging in cybersecurity practices when better informed about the risks (mean = 4.10). The need for enhanced education and awareness campaigns was also rated highly (mean = 3.71). However, confidence in identifying and responding to sophisticated threats after education and awareness training received the lowest mean in this group (2.64). These findings indicate that respondents were receptive to cybersecurity education but may need more practical and continuous learning activities rather than one-time information campaigns.

Indicator	Mean	Descriptive Equivalent	Rank
Lack of public understanding of	3.40	Moderately Aware	2

malware and masquerading			
Need for enhanced education and awareness campaigns	3.71	Highly Aware	3
Likelihood of engaging in cybersecurity practices when better informed	4.10	Highly Aware	1
Belief that current educational efforts raise public awareness	3.13	Moderately Aware	4
Confidence after education and awareness training	2.64	Moderately Aware	5
Overall Mean	3.39	Moderately Aware	—

4.4 Perception of Permission-Based Detection:

Perception of permission-based detection obtained an overall mean of 3.41, indicating agreement with the usefulness of this approach. The highest-rated indicator was the belief that permission-based detection can protect personal data and privacy (mean = 3.92). Respondents also agreed that they were more likely to avoid applications whose requested permissions appeared unnecessary (mean = 3.84), and they agreed that permission-based detection can identify potentially malicious applications (mean = 3.53). However, attention to permissions before installation received 2.87 and confidence in distinguishing legitimate from malicious applications received 2.90. This gap between favorable perception and actual decision confidence is important because it suggests that users may understand the value of permission-based detection without consistently applying it in practice.

Indicator	Mean	Descriptive Equivalent	Rank
Permission-based detection is effective in identifying potentially malicious applications	3.53	Agree	3
Attention to permissions requested before installation	2.87	Neutral	5
Likelihood of avoiding applications with unnecessary permissions	3.84	Agree	2
Permission-based detection protects personal data and privacy	3.92	Agree	1
Confidence in distinguishing legitimate and malicious applications	2.90	Neutral	4
Overall Mean	3.41	Agree	—

Nexus Global Research Journal of Multidisciplinary
Journal Homepage: https://nexusglobalresearch.com/journal/ngrjm/

4.5 Perception of Anomaly-Based Detection:

Anomaly-based detection obtained an overall mean of 3.82, interpreted as Agree. The highest-rated indicator was the belief that anomaly detection is reliable for identifying unusual application behavior (mean = 4.30), followed by the belief that it provides confidence when using mobile applications (mean = 4.20). Respondents also agreed that it can identify potential masquerade attacks (mean = 4.10) and distinguish normal from abnormal behavior (mean = 3.80). The lowest-rated indicator concerned awareness of the signs monitored by anomaly detection (mean = 2.70). Thus, respondents expressed confidence in the technology while showing less understanding of the specific behaviors and indicators it monitors.

Indicator	Mean	Descriptive Equivalent	Rank
Anomaly detection is reliable for detecting unusual application behavior	4.30	Strongly Agree	1
Anomaly detection can identify potential masquerade attacks	4.10	Agree	3
Awareness of signs monitored by anomaly detection	2.70	Neutral	5
Anomaly detection can distinguish normal from abnormal behavior	3.80	Agree	4
Anomaly detection provides confidence when using mobile applications	4.20	Strongly Agree	2
Overall Mean	3.82	Agree	—

4.6 Development of the MAPER Framework:

The empirical findings provided the basis for developing the researcher-developed MAPER Framework. The respondents were moderately aware of Android malware and masquerade attacks, while their confidence in understanding masquerade attack techniques was low. At the same time, they showed a strong willingness to engage in safer cybersecurity practices when better informed and favorable perceptions of both permission-based and anomaly-based detection. These findings indicate that a useful mitigation approach should combine technical controls with user-centered measures.

Component	Purpose	Core Actions
M – Monitor	Identify changes in application and device behavior that may indicate malware or masquerade attacks.	Review battery and data usage, application activity, unexpected overlays, new permission requests, login prompts, and security alerts.
A – Assess	Determine whether an application or activity is legitimate and	Verify application source, developer information, package identity, permissions, digital

*Corresponding Author: Wens Zaren P. Duron, Email: rvcabansag14@gmail.com
Received: 03 Aug 2026 | Accepted: 16 Aug 2026 | Published: 20 Aug 2026

	consistent with its intended purpose.	signatures when available, and behavior.
P – Prevent	Reduce opportunities for malware infection and unauthorized application installation.	Use trusted sources, update Android devices, enable built-in security features, review permissions, and implement organizational policies.
E – Educate	Strengthen users' cybersecurity awareness, knowledge, and decision-making.	Conduct orientations, awareness campaigns, demonstrations, simulations, case-based learning, permission-awareness sessions, and microlearning.
R – Respond	Contain security incidents quickly and support recovery while preventing recurrence.	Report incidents, remove malicious applications, revoke unnecessary permissions, reset compromised credentials, preserve evidence, when necessary, document incidents, and review lessons learned.

The Monitor component addresses the need to identify suspicious changes in application and device behavior. The Assess component emphasizes verification of application legitimacy through source, developer information, package identity, permissions, and behavior. The Prevent component focuses on trusted sources, software updates, built-in security features, permission management, and organizational policies. The Educate component responds directly to the moderate awareness results and the strong willingness of respondents to adopt safer practices when better informed. The Respond component completes the mitigation cycle by providing actions after suspicious or malicious activity is identified.

The MAPER Framework is not presented as an adopted framework from a single source. It represents the researcher's synthesis and organization of security principles identified in the reviewed literature and the empirical findings of the study. Its contribution lies in integrating monitoring, assessment, prevention, education, and response specifically for Android devices used within an aviation training environment.

5. CONCLUSION:

The study found that aviation training device users had moderate awareness of Android malware, masquerade attacks, and public education and interventions. Although respondents recognized the potential risks associated with mobile threats, the results revealed limitations in their confidence, threat recognition, and preparedness to respond. The strongest awareness-related finding was the respondents' willingness to engage in cybersecurity practices when better informed, indicating a positive opportunity for continuous and practical cybersecurity education.

Respondents also demonstrated favorable perceptions of permission-based and anomaly-based detection. Permission-based detection was viewed as useful for protecting personal data and privacy, while anomaly-based detection was viewed favorably for identifying unusual behavior and potential masquerade attacks. However, the lower ratings related to understanding permission requests and anomaly indicators show that technology should be accompanied by user education and practical guidance.

Based on these findings and the reviewed literature, the researcher developed the MAPER Framework—Monitor, Assess, Prevent, Educate, and Respond. The framework provides an integrated approach that combines technical safeguards, user awareness, preventive practices, assessment procedures, and incident response. It is intended as a context-specific guide for strengthening cybersecurity practices involving Android devices used in aviation training.

6. RECOMMENDATIONS:

1. Aviation training organizations should consider adopting the researcher-developed MAPER Framework as a guide for strengthening cybersecurity practices involving Android devices used for training and access to technical resources.

2. The Technical Training Department and IT Department should collaborate in implementing cybersecurity awareness activities, safe mobile-device practices, application permission management, security monitoring, and incident reporting procedures.

3. Cybersecurity awareness programs should be conducted regularly rather than as one-time activities. Training should include recognition of Android malware, identification of masquerade attacks, evaluation of application permissions, verification of legitimate applications, and appropriate response to suspicious activities.

4. Training device users should practice safer mobile-device behaviors by reviewing application permissions, using trusted application sources, maintaining updated software and security features, and reporting suspicious applications or activities.

5. Future researchers should validate and improve the MAPER Framework by implementing and evaluating it in other aviation training organizations and educational institutions to determine its effectiveness and applicability.

6. Future studies may explore adaptation of the framework to other mobile operating systems, including iOS, and examine whether similar mitigation principles can be applied to broader mobile-security environments.

7. Long-term studies should examine the impact of the MAPER Framework on cybersecurity awareness, mobile-security practices, incident-response capabilities, and the protection of training materials, technical manuals, maintenance records, and other organizational information.

7. ETHICAL CONSIDERATIONS:

The study observed informed consent, voluntary participation, privacy, confidentiality, and responsible data handling. Respondents were informed about the purpose and general procedures before participation and could decline or discontinue participation without penalty. Responses were used for academic research purposes and reported in aggregate form. The study did not require direct access to respondents' devices and did not request passwords, authentication codes, private communications, personal files, or application contents. The research design did not expose participants to malware and did not require the installation of security software for research purposes.

8. REFERENCES:

- Aonzo, S., Georgiu, G. C., Verderame, L., & Merlo, A. (2020). Obfuscapk: An open-source black-box obfuscation tool for Android apps. IEEE Security & Privacy, 18(3).
- Aso, A., Ono, M., & Yoshida, T. (2018). Mobile malware: A survey on security threats and countermeasures. IEEE Access, 6, 66325–66340.
- Chen, J., Xue, Y., Chen, Y., Tian, K., Jia, W., & Liu, B. (2019). Understanding user behavior of Android app installation. IEEE Transactions on Mobile Computing, 18(3), 593–606.
- Chiew, K. L., et al. (2023). Mitigation strategies against phishing attacks: A systematic literature review. Computers & Security, 132, 103387.
- Ehsan, A., Catal, C., & Mishra, A. (2022). Detecting malware by analyzing app permissions on Android platform: A systematic literature review. Sensors, 22(20), 7928.
- Fernandez, E. B., Camacho, D. T., & Gonzalez, R. C. (2018). A framework for mobile security awareness in the Philippines. 2018 IEEE 9th International Conference on Humanoid Robotics (Humanoids), 83–88.
- Kim, H., & Lee, J. (2020). Effectiveness of mobile security awareness programs in

educational settings. Journal of Information Security, 14(3), 150–164.

- Lahcen, R. A. M., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity.
- Lee, S. U.-J., & Oh, J. (2021). An empirical study on the impact of permission smell in Android applications. Journal of the Korea Society of Computer and Information, 26(6), 89–96.
- Mirza, M., et al. (2021). MapperDroid: Verifying app capabilities from description to permissions and API calls. Computers & Security, 111, 102493.
- Pan, et al. (2020). The capstone literature review identifies preventive measures, behavioral monitoring, application analysis, and regular security updates as complementary Android malware mitigation measures.
- Parayno, J. G., & Lim, C. S. (2020). An empirical assessment of mobile malware detection in the Philippines. International Journal of Electrical and Computer Engineering, 14(3), 1021–1028.
- Rahima Manzil, H. H., & Naik, S. M. (2024). Detection approaches for Android malware: Taxonomy and review analysis. Expert Systems with Applications, 237, 122255.
- Ramnath, R., & Kuriakose, A. (2019). Mobile technologies for teaching and learning. In Handbook of Mobile Teaching and Learning.
- Saher, et al. (2021). The capstone literature review emphasizes technical controls, organizational policies, and continuous assessment for Android security.
- Senanayake, J., Kalutarage, H., & Al-Kadri, M. O. (2021). Android mobile malware detection using machine learning: A systematic review.
- Singh, P., Bhattacharjee, S., & Singh, K. (2023). Region-specific training data in machine learning-based malware detection: A case study. Journal of Computer Applications, 184(1), 15–30.
- Wang, L., Chen, X., & Zhang, Y. (2022). Improving students' cybersecurity preparedness through simulated cyber attack scenarios. Computers & Security, 112, 102524.
- Wang, W., Li, Y., Wang, X., Liu, J., & Zhang, X. (2017). Detecting Android malware through system call sequences. IEEE Access, 5, 17403–17411.
- Weichbroth, P. (2020). The capstone literature review emphasizes continuous cybersecurity awareness and safer user behavior.
- Zhou, Y., & Zhou, Y. (2012). A survey of mobile malware and countermeasures. Journal of Computer Security, 20(2), 215–239.