

Malicious APK Distribution via WhatsApp and Its Effects on User Security and Privacy

Mr. Pranav Eknath Kanawade

pranavkanawade2003@gmail.com

MCS Student

Dr. D. Y. Patil Arts, Commerce & Science College

Mr. Akash Dagadu Kolekar

akashkolekar831@gmail.com

MCS Student

Dr. D. Y. Patil Arts, Commerce & Science College

Mr. Shubham Vilas Shelke

Shubhamshelke173@gmail.com

MCS Student

Dr. D. Y. Patil Arts, Commerce & Science College

Abstract: This study explores the growing threat of malicious APK (Android Package Kit) files that are distributed through WhatsApp and their impact on user security and privacy. With billions of users worldwide, WhatsApp has become an easy and fast medium for cybercriminals to spread harmful files. These APKs are often disguised as useful or attractive applications, such as free premium apps, modified software, or fake updates, which trick users into installing them.

Once installed, these applications can lead to serious consequences including identity theft, malware infections, financial loss, and unauthorized access to personal data. The research uses a mixed-method approach, including surveys and analysis of user awareness, distribution patterns, and attack techniques.

The findings show that many users unknowingly install APK files from untrusted sources, exposing their devices to risks like spyware, keylogging, and data theft. The problem is worsened by low cybersecurity awareness, trust in forwarded messages, and lack of verification practices. The study highlights the need for awareness programs, better detection systems, and preventive measures such as verifying sources and using antivirus tools.

Keywords: Malicious APK, WhatsApp, Cybersecurity, Data Privacy, Mobile Threats, User Awareness, Spyware, Social Engineering

Introduction

Mobile applications have become an essential part of everyday life, handling tasks such as communication, banking, and entertainment. Android, being the most widely used mobile operating system, is a major target for cyber threats due to its open nature.

Android applications are distributed as APK files, which allow easy installation and updates. However, Android also allows installation from external sources (side-loading), which creates opportunities for attackers to distribute harmful applications.

WhatsApp is widely used for communication and provides end-to-end encryption, which sometimes creates a false sense of safety. Cybercriminals exploit this platform to send malicious APK files disguised as attractive offers like free subscriptions, modified apps, or game hacks.

Once installed, these APKs can steal personal data, track user activity, or perform financial fraud such as capturing OTPs. A major issue is that users often trust files shared by friends or contacts without verifying them. This “trust chain” makes users more vulnerable, especially those with less technical knowledge.

This situation highlights the urgent need for awareness and preventive strategies to protect users from such threats.

Statement of the Problem:

The rapid growth of smartphone usage and messaging platforms such as WhatsApp has significantly increased the risk of cyber threats, particularly through the distribution of malicious APK files. These files are often shared in the form of attractive offers, modified applications, or fake updates, making them difficult for users to identify as harmful.

A major concern is that many users download and install APK files from unverified sources, bypassing the security mechanisms provided by official platforms like the Google Play Store. This behaviour exposes users to serious risks, including data theft, financial fraud, unauthorized access, and malware infections.

Despite having basic awareness about cybersecurity threats, users often fail to follow safe practices such as verifying the source of applications or using security tools. The trust placed in forwarded messages from known contacts further increases vulnerability, as users tend to assume that shared files are safe.

Therefore, the core problem addressed in this study is the gap between user awareness and actual behaviour regarding APK file installation, and how this gap contributes to increased security and privacy risks. Addressing this issue is essential to reduce cyber threats and promote safer digital practices among smartphone users.

Objectives of the study:

The specific objectives are as follows:

- To analyze how frequently users receive APK files through messaging applications.
- To evaluate the level of user awareness about APK files and their potential security risks.
- To identify common user behaviours related to downloading and installing APK files from unknown sources.
- To investigate the types of security issues experienced after installing such files, including data breaches and financial fraud.
- To assess the security practices followed by users to protect their devices.
- To highlight the gap between awareness and actual security behaviour among users.
- To emphasize the need for cybersecurity education and awareness programs.

Literature Review:

With the rapid growth of smartphone usage and mobile applications, the distribution of Android application packages (APKs) through unofficial channels has increased significantly. Several studies have highlighted the security risks associated with installing APK files from unknown or untrusted sources.

Research in the field of mobile security indicates that third-party APK files are one of the major sources of malware infections in Android devices. Unlike applications downloaded from official platforms such as the Google Play Store, APK files shared through messaging applications bypass standard security checks, making them more vulnerable to malicious modifications.

Previous studies have shown that many users lack sufficient awareness about the risks involved in installing APK files. Even when users are aware of potential threats such as malware, spyware, and phishing attacks, they often prioritize convenience over security. This behaviour increases the likelihood of cyber incidents, including unauthorized data access, financial fraud, and device compromise.

According to existing literature, messaging platforms like WhatsApp play a significant role in the spread of APK files. The trust factor between users often leads individuals to download and install files without proper verification. Researchers have also pointed out that attackers exploit social engineering techniques to distribute harmful APKs by disguising them as useful or popular applications.

Furthermore, studies emphasize that while basic security practices—such as avoiding unknown sources—are commonly known, advanced measures like verifying app permissions, checking developer credibility, and using antivirus tools are less frequently adopted. This gap between knowledge and actual behaviour is a recurring theme across multiple research works.

Recent literature also stresses the importance of integrating cybersecurity awareness into educational systems. Educating users about safe digital practices, potential threats, and preventive measures can significantly reduce the risks associated with APK file installations.

Research Methodology

This study used a mixed-method approach combining both qualitative and quantitative techniques.

- A structured survey was conducted using Google Forms
- Participants included 100–150 smartphone users who actively use WhatsApp
- Questions included multiple-choice and Likert scale formats
- Data was analysed using MS Excel for charts and interpretation
- Reports were prepared using MS Word

Participation was voluntary, and user data was kept confidential to maintain ethical standards.

Data Analysis and Discussion

The survey results reveal a noticeable trend of widespread exposure to APK files along with a gap between user awareness and actual behaviour.

Exposure and Installation Patterns

The collected data indicates that a large number of participants (82.4%) frequently receive different types of files through WhatsApp. Among them, 53.9% reported receiving APK files from unknown or untrusted sources, which raises serious security concerns. Additionally, 46.6% of respondents stated that either they or someone they know experienced problems such as device compromise, data loss, or financial scams after installing such APK files. This clearly shows that malicious APK distribution is leading to real-life negative outcomes.

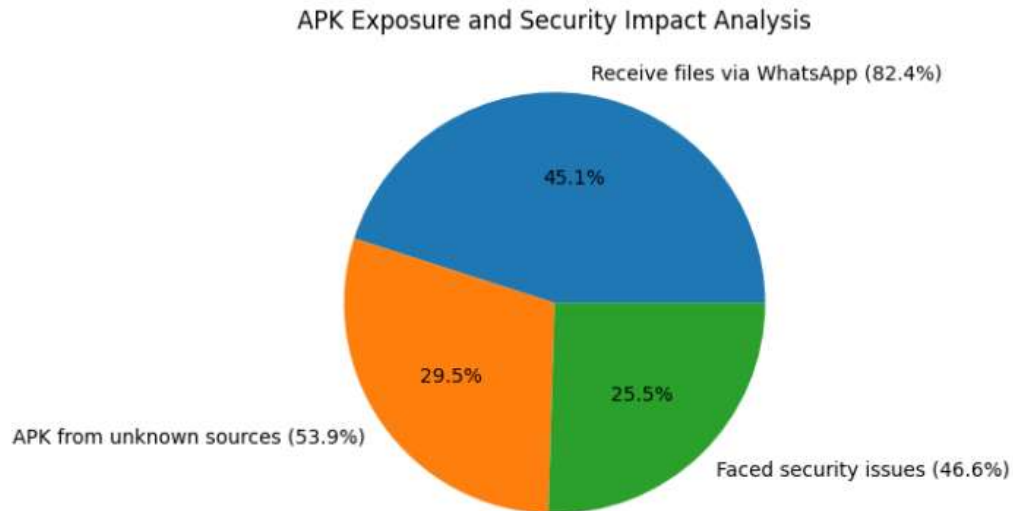
User Awareness and Risk Perception

A majority of users (77.5%) are familiar with the term “APK,” and 69.6% understand that such files may contain harmful elements like malware or spyware. Despite this awareness, safe practices are not consistently followed. When asked about risks, most respondents identified personal data theft (48.5%) and financial fraud (31.1%) as major concerns. However, behavior does not always align with this knowledge. For instance, 15.5% of users admitted they would install an APK received from a trusted contact without verification, showing dependence on trust rather than security checks.

Security Practices and Educational Gap

The most commonly followed safety practice is avoiding downloads from unknown sources (60.2%). However, only a small percentage of users adopt technical security measures such as

antivirus tools (13.6%) or verifying the developer/source (13.6%). This suggests that users rely more on basic caution instead of advanced protection methods. Importantly, 78.6% of participants believe that cybersecurity awareness should be included in educational institutions, highlighting the need for formal training in digital safety.



Findings

The study reveals the following key points:

- **High Exposure:** Many users receive APK files from unknown sources
- **Real Impact:** Nearly half of users face or know someone affected by security issues
- **Awareness Gap:** Users know risks but do not follow safe practices
- **Low Technical Protection:** Very few use antivirus or verification methods
- **Need for Education:** Strong demand for cybersecurity awareness programs

Suggestions

To reduce risks, the following measures are recommended:

1. Verify Sources

Users should install apps only from trusted platforms and verify developers.

2. Cybersecurity Education

Institutions should include awareness programs on mobile security.

3. Use Antivirus Tools

Encourage users to scan APK files before installation.

4. Platform Improvements

Messaging apps should improve detection of suspicious files and links.

5. Reporting Mechanism

Users should report suspicious APKs to authorities or security teams.

Future Scope:

The findings of this study open several opportunities for further research and development in the field of mobile security and user awareness.

In the future, this research can be extended by developing advanced detection systems that can automatically identify malicious APK files before installation. Integration of machine learning and artificial intelligence techniques can help in analysing application behaviour and detecting potential threats in real time.

Another important area for future work is the design and implementation of user-friendly security tools or mobile applications that can warn users about unsafe APK files received through messaging platforms. These tools can provide risk assessments and guide users in making secure decisions.

Further studies can also focus on a larger and more diverse population to gain deeper insights into user behavior across different regions, age groups, and educational backgrounds. This would help in creating more targeted cybersecurity awareness programs.

In addition, future research can explore the effectiveness of educational interventions, such as workshops or curriculum-based cybersecurity training, in improving user behavior and reducing risky practices.

There is also scope to collaborate with messaging platforms like WhatsApp and official app distribution services such as Google Play Store to implement stricter security mechanisms that can detect and block the sharing of harmful APK files.

Overall, continued research and innovation in this area can contribute to building a safer digital environment and minimizing the risks associated with unauthorized application installations.

Conclusion

This research confirms that malicious APK files shared through WhatsApp pose a serious threat to user security and privacy. A large number of users are exposed to such risks, and many have already experienced negative consequences.

Although users have some level of awareness, they often fail to follow proper safety practices. The main issue lies in the misuse of trust within messaging platforms.

To address this problem, a combined effort is required from users, educational institutions, and technology platforms. Promoting awareness, improving technical measures, and encouraging responsible behaviour can help create a safer digital environment.

References

1. Google. (2023). Protect your device from harmful apps (Play Protect). Google Play Help. Retrieved from <https://support.google.com/googleplay/answer/2812853>
2. WhatsApp. (2023). Security and Privacy Features on WhatsApp. WhatsApp Help Center. Retrieved from <https://www.whatsapp.com/security>
3. Kaspersky. (2023). Malicious APK files: How to stay safe when installing Android apps. Kaspersky Security Blog. Retrieved from <https://www.kaspersky.com/blog/malicious-apk-files>
4. Symantec (NortonLifeLock). (2022). Mobile Malware Report: The Rising Threat of Android APK Scams. Norton Cyber Safety Insights.
5. Check Point Research. (2023). Fake and malicious Android apps distributed via messaging platforms. Retrieved from <https://research.checkpoint.com>
6. Avast Software. (2023). Android Malware and Fake Apps: How Cybercriminals Trick Users into Installing Malicious APKs. Avast Security Blog. Retrieved from <https://blog.avast.com>
7. Palo Alto Networks Unit 42. (2022). The Evolution of Android Malware: Threats and Attack Vectors. Palo Alto Networks Report.
8. Kumar, S., & Singh, A. (2021). Analysis of Android Malware and its Distribution Through Social Platforms. *International Journal of Computer Applications*, 183(22), 15–20. <https://doi.org/10.5120/ijca2021921802>
9. Jain, P., & Bansal, R. (2022). Understanding User Awareness towards Mobile Application Security in India. *Journal of Information Security and Applications*, 68, 103316. <https://doi.org/10.1016/j.jisa.2022.103316>
10. CERT-In (Indian Computer Emergency Response Team). (2023). Advisory on Fake and Malicious Mobile Applications Distributed via Messaging Apps. Government of India. Retrieved from <https://www.cert-in.org.in>