

Securing user data in mobile application development: review and case study

Andrej Pavešić, Renata Mekovec

University of Zagreb Faculty of Organization and Informatics

Pavlinka 2, 42000 Varaždin, Croatia

apavesic22@student.foi.hr, renata.mekovec@foi.unizg.hr

Abstract. *This paper examines recent advances in mobile app development research and analyzes practices employed by developers to ensure user data security. Utilizing bibliometric analysis—specifically performance analysis and science mapping—we identify emerging trends and examine the domain's intellectual structure. Additionally, the paper outlines critical security threats confronting developers and users. A qualitative case study examines BetterHelp, MyFitnessPal, and Noom—three popular Android health apps handling sensitive medical and personal data that raise privacy concerns. The investigation employs qualitative comparative content analysis alongside platform-specific technical examinations.*

Keywords. Mobile application, self-regulation, data protection

1 Introduction

Mobile applications serve as a primary channel for accessing digital content and services. Since smartphones are personal devices, they fall under the category of intimacy and privacy for their owners. Therefore, it is imperative for individuals to manage the data accessible to mobile applications. Sensor Tower states that the average person spent 3.6 hours a day on their mobile phone last year and uses 10 apps each day (SensorTower, 2026). While users have over 80 apps on average (roughly 62% of those are unused) the majority of a user's time (up to 90%) is spent in a select few key categories: social media, communication, and entertainment (Raas Cloud, n.d.).

Mobile apps are increasingly used by users for daily tasks, however processing personal data through them raises security and privacy problems. The variety of data and sensors in mobile devices, the use of different identifiers and the possibility of users being tracked, the complex mobile app ecosystem and app developers' limitations, and the extensive use of third-party software and services pose such risks. Mobile apps confront significant problems in implementing the GDPR's key data protection standards. This may prevent mobile app developers and suppliers from complying with GDPR standards on transparency and

consent, data protection by design and default, and processing security (ENISA, 2017). Stakeholders engaged in the development of mobile applications must guarantee adherence to data protection obligations and the rights of users (CNIL, 2025). Identifying the privacy and data protection risks for individuals associated with mobile app usage necessitates an understanding of the processing context to identify risk sources, assess the potential impact on individuals, and recognize the constraints in implementing measures to mitigate those risks (World Intellectual Property Organization, 2021). Bian et al. reported that on average, an app collects 24 data items across 16 types, with 70% used for purposes unrelated to core functionality—most often analytics and developer advertising or marketing (Bian et al., 2022).

Organizations that create mobile applications must comply with requirements such as the GDPR and corresponding national legislative frameworks. However, within the application development process, enterprises have some flexibility in establishing internal rules and standards to improve personal data security and privacy. Such sets of ethical principles and operational rules are known as Codes of Conduct, and they are encouraged by Article 40 of the GDPR since they help to ensure its proper implementation.

The aim of this paper is to investigate current trends in research related with mobile app development, as well as to analyse practice used by mobile apps developers to secure the process of users' data maintenance. This paper addresses two research questions:

R1: What key security challenges are currently explored in mobile application development research?

R2: What mechanisms do mobile applications employ to secure user data?

The paper is structured as follows. The second section presents state of research in the domain of mobile apps using a bibliometric analysis. Third section presents codes of conduct as a self-regulation instrument that can be used in process of development of mobile apps. Fourth section introduces the most common security risks and vulnerabilities of mobile applications. Fifth section presents results of comparative analysis of three mobile application

regarding their users' data collection and usage practice.

2 State of research in domain

In order to identify the most important studies on security risks connected with mobile application we employed a publication-related metrics and co-word analysis following the steps of the bibliometric analysis procedure (Donthu et al., 2021). The articles included in the analysis were retrieved from the Scopus database. This database was chosen because it contains the most recent full-text peer-reviewed publications and database research resulted with the maximum number of articles. The following keywords were used in a keywords-based search method: ("security" AND "risk*" OR "vulnerabilities") AND ("mobile" AND "applications" OR "app*"). Articles were selected if the terms defined in the search query appeared in the titles, abstracts, or keywords. Furthermore, no time frame was specified, allowing for a comprehensive coverage of the entire discourse on topic. The literature search was conducted on 1 June 2026. The result was 546 articles presented in Fig. 1.

From 1999 to 2026, the graph displays a long-term increasing tendency in the quantity of papers, which may be broken down into three major stages. Less than five documents are produced annually during the first phase, which runs from 1999 to 2010. Thereafter, there is an increase that happens in waves, peaking in 2014 and again in 2019 with more than 40 documents. This is followed by a brief fall in 2020. The final stage is characterized by rapid, nearly exponential expansion, reaching a peak of about 85 documents in 2025. These two waves can be connected with the amendment of two important regulations, Regulation (EU) 2016/679 (GDPR) (European Parliament and the Council of the European Union, 2016) and the NIS Directive Network

and Information Systems Directive) as foundational of cybersecurity legislation. The original NIS Directive was adopted in 2016. However, it was significantly updated by NIS2 (Directive (EU) 2022/2555) (European Parliament and the Council of the European Union, 2022).

In the second step, a science mapping technique is utilized to locate the most significant authors in the domain. The quantity of citations of the publications was taken into account while selecting important papers, and some of the most widely referenced articles in our study (Table 1). Based on the bibliometric data, the analyzed papers exhibit a high citation impact, with citations ranging from 465 to 847, indicating their significant influence on the mobile application research domain. The study by Chin et al. (2021) on inter-application communication in Android stands out as the most prominent work in the dataset, accumulating the highest number of citations (847).

The data reveals a strong research focus on mobile security and user privacy, which comprises four out of the five top-cited papers, while health-related mobile applications (m-Health) also represent a highly impactful niche.

Fig. 2 displays a keyword co-occurrence map of selected articles derived by bibliometric analysis in VOSViewer. In the network visualization, items are represented by their label and by default also by a circle. The size of the label and the circle of an item is determined by the weight of the item. The higher the weight of an item, the larger the label and the circle of the item. The colour of an item is determined by time overlay. The focus of vulnerability analysis has matured over time. Traditional themes like 'risk assessment' and 'authentication' (blue/teal) have evolved into domains such as 'cyber-physical systems' and 'app-in-app ecosystem' security vulnerabilities, which represent the latest research frontiers heading into 2026.

Documents by year

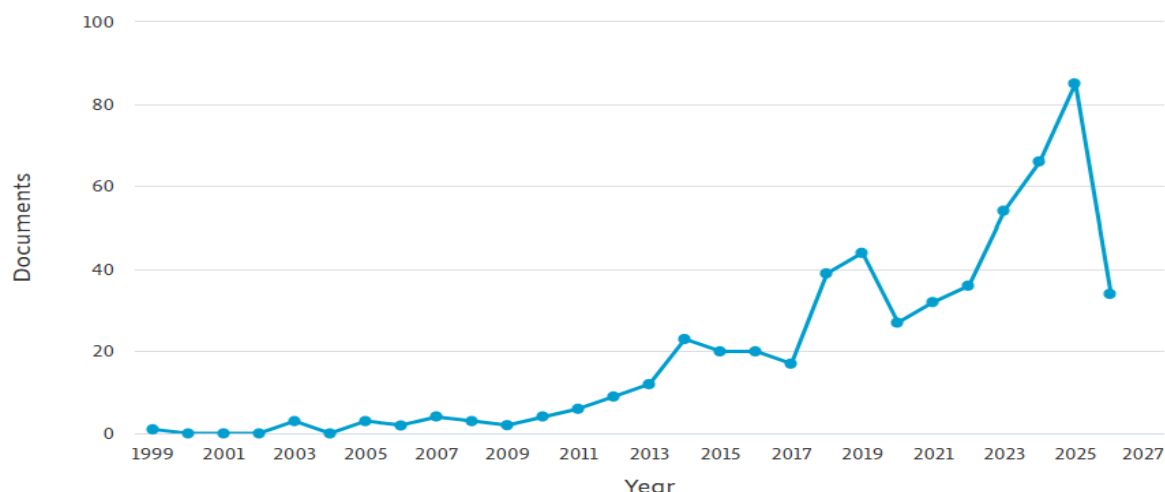


Figure 1. Number of articles by year

guidelines is to describe how major technology firms (referred to as gatekeepers or access controllers, including Google, Meta, and Apple) can fulfil their competition-related obligations mandated by the DMA while remaining compliant to the stringent privacy and data protection regulations established by the GDPR.

4 Security risks and vulnerabilities of mobile applications

Security vulnerabilities most often do not arise from structural errors within the operating system itself, but rather from developers' carelessness in implementing security protocols or sophisticated methods used by attackers to deceive the end user. Threats are constantly evolving, and those who create them are continually finding new ways to cause damage or collect unauthorized data. Kaspersky Lab conducted a study on the prevalence of mobile malware in the second quarter of 2023 and the second quarter of 2025 by type of malware (Statista, 2025.). At the very beginning of the observed period, RiskTool was identified as the most prevalent threat. Although it is not a malicious program in the classical sense, it is a legitimate application whose functionality can be misused by attackers to compromise the system. AdWare (advertising malware) recorded a sharp increase in prevalence from the second to the third quarter of 2023. AdWare is most often installed with seemingly free applications, after which it displays ads in an invasive manner and secretly collects metadata about the user, such as interests and location, without their consent. The decline in the prevalence of AdWare began a trend of growth in the prevalence of banking Trojans (Trojan-Banker), its primary goal is to steal users' financial data. It most often arrives on a device through the installation of unofficial and compromised copies of popular software or as attachments in phishing emails. The main goals of this malware are to intercept sensitive information by monitoring keystrokes (keylogging), finding passwords stored within the file system, or displaying fake interfaces (overlays) for entering banking information. In addition to direct financial damage, these programs also enable the theft of the victim's identity (Point, 2026.)

A Trojan-Spy represents a specific type of malicious software whose primary goal is unauthorized

monitoring of users and data collection without their consent. While the user believes that he is using a standard and harmless application, this program secretly collects a wide range of information in the background. Unlike bank Trojans that are narrowly focused on finance, the spy variant indiscriminately collects all available data – from private messages and call history to sound recording via microphone or location tracking (Threat, 2026.) In the first quarter of 2025, the share of this threat was a high 20.24%, which made it the second most represented type of malicious software. However, the latest data from the second quarter of 2025 indicate a dramatic reversal; the prevalence of this malware dropped to only 2.61%. Other malicious programs are represented to a much lesser extent, but it is significant that most of them are based on some variant of a Trojan, whether it is a Trojan-Dropper, Trojan-Downloader or Trojan-SMS distribution.

4.1 Context of security risks

The most important security threats that developers and users must deal with are identified and ranked by the OWASP Mobile Top 10 project (2026). First published in 2016, the study was updated in 2024 to take into account contemporary technical issues. Data from these two eras can be compared to gain insight into how security threats have changed and how mobile application protection has evolved. This evolution is presented directly in Fig. 3. The modern threat landscape introduces a strong emphasis on data governance and integration ecosystem vulnerabilities. Some new threats emerge such as inadequate supply chain security (M2) and inadequate privacy controls (M6) which demonstrates that contemporary mobile applications face risks far beyond local code execution. Besides that, the most important risk which emerged as completely new is the risk of improper credential usage (M1). This threat by itself can result in automated attacks if the credentials are hardcoded and identified by the attackers as well as other weaknesses caused by improper credential usage.

Furthermore, the structural reordering reveals that traditional vulnerabilities have matured, altering their critical prioritization.

Comparison Between 2016-2024		
OWASP-2016	OWASP-2024-Release	Comparison Between 2016-2024
M1: Improper Platform Usage	M1: Improper Credential Usage	New
M2: Insecure Data Storage	M2: Inadequate Supply Chain Security	New
M3: Insecure Communication	M3: Insecure Authentication / Authorization	Merged M4&M6 to M3
M4: Insecure Authentication	M4: Insufficient Input/Output Validation	New
M5: Insufficient Cryptography	M5: Insecure Communication	Moved from M3 to M5
M6: Insecure Authorization	M6: Inadequate Privacy Controls	New
M7: Client Code Quality	M7: Insufficient Binary Protections	Merged M8&M9 to M7
M8: Code Tampering	M8: Security Misconfiguration	Rewording [M10]
M9: Reverse Engineering	M9: Insecure Data Storage	Moved from M2 to M9
M10: Extraneous Functionality	M10: Insufficient Cryptography	Moved from M5 to M10

Figure 3. OWASP comparison of top 10 mobile risks in 2016 and 2024 (OWASP 2026)

For instance, fundamental structural issues like insecure data storage (M2 in 2016) and insecure communication (M3 in 2016) have been downgraded to lower priority slots (M9 and M5 in 2024). This shift doesn't imply that these threats are obsolete but rather that security of operating systems have improved which changed the developer's focus primarily on authentication mechanics, credential lifecycle management and validation layers.

Additionally, the unification of older separate categories - such as merging 2016's distinct authentication and authorization threats into a singular 2024 entry (M3) which reflects a more unified approach to defending digital endpoints.

5 Case study

This section presents a qualitative case study analyzing three widely used mobile health applications on Android: BetterHelp (v3.05), MyFitnessPal (v26.27.0) and Noom (v14.26.0). These specific platforms were selected because they process highly sensitive medical and personal data which raises major privacy and security concerns. To ensure a standardized assessment, the case study utilizes a qualitative comparative content analysis combined with a platform-specific technical review. The data is gathered from two primary sources: the official Privacy Policies of the applications and their permission manifests available on the Google Play store. To ensure the empirical reproducibility of the study, all technical evaluations were conducted under a standardized protocol between June 26, 2026 and June 28, 2026. The primary testing environment was deployed in Croatia. Testing was carried out on physical reference hardware: a Xiaomi 15T Pro running an unrooted, clean instance of Android 16.

5.1 Methodology and evaluation criteria

The testing procedure followed a four step protocol: inspecting requested Android permissions and Google Play store disclosures, executing initial launch to log mandatory registration walls, cookie banners and profiling questionnaires prior to account setup, systematically denying requested dangerous permissions and finally navigating settings menus to test the actual availability of data control. Furthermore, this research is structured around four distinct data privacy and security criteria which are all based on previously explained testing procedure: dangerous permissions, granular permission control, third-party SDK disclosure and in-app data privacy controls. These specific criteria were established to bridge the gap between developer self-regulation and the practical security risks inherent to the Android operating system and because codes of conduct often provide theoretical frameworks for data privacy while they often lack the technical enforcement mechanisms.

The dangerous permissions criterion examines whether the application requests access to sensitive Android system resources which could reveal sensitive personal data and compromise user privacy if mismanaged. It will be graded on a three-tier qualitative scale: high, medium and low. "High" indicates that the application requests access to 2 or more highly sensitive system vectors (e.g. precise location, biometric sensors, system storage etc.). "Medium" strictly represents transactional, session-based and user-initiated dangerous permissions (e.g. runtime hardware access to camera and recording audio during active user interactions). "Low" is assigned if the application requests minimal or no system permissions beyond basic internet access.

Table 2. Results of comparative analysis

Criteria	BetterHelp	MyFitnessPal	Noom
Dangerous permissions	Medium	High	High
Granular permission control	Yes	Yes	Yes
Third-party SDK disclosure	Disclosed	Disclosed	Disclosed
In-app data privacy control	Yes	Yes	Partial

Granular permission control is a second criterion which examines whether the application remains fully functional after the user's denial of mentioned dangerous permissions. This criterion will be graded with a simple "yes" if core features remain stable without access to restricted resources or "no" statement if it is the opposite.

Third-party SDK disclosure criterion investigates if the application's official documentation transparently lists the integration of external SDK-s used for analytics or marketing. It will be graded either as a "disclosed" if the specific partners for telemetry and marketing were named or a "undisclosed" if they weren't named.

Finally, the in-app data privacy controls criterion evaluates whether the user interface provides an explicit option allowing users to manage their optional data sharing. This criterion is measured across three levels: yes, partial, or limited. A "yes" grade requires a dedicated, easily accessible privacy dashboard or toggle within the application interface. "Partial" indicates that options exist but are split across complex sub-menus, while "limited" means the application offers no native toggles, forcing users to rely entirely on general Android operating system settings to restrict tracking.

6 Discussion of results

After applying the established methodology and criteria to the selected applications the results were structured and summarized in Table 2. By applying a case study and comparative analysis approach, the findings reveal substantial variations in how mHealth applications use and process user data. Applications mostly behave in accordance with industry standards while some of the results show that certain things can and should be changed in order to improve user autonomy and privacy.

Upon initial execution, the BetterHelp application captures immediate cookie consent before any other user interaction. However, before it allows the user to provide an e-mail address or login credentials it gathers user data by presenting questions regarding biological age, sexual orientation, religious affiliations and

relationship status among other variables. This data is extracted

in order to construct a user profile prior to the formal creation of the account. Regarding the dangerous permissions criterion the platform is graded as medium because it avoids tracking background biometric data. Only dangerous permissions that can be requested are access to camera and microphone for live video and audio therapy sessions. Granular permission control is graded as yes because users are not obliged to communicate with therapists through video calls as they can be communicating with simple text messages. Therefore, the core functionality of the application stays functional even after denying the access to camera and microphone. Furthermore, BetterHelp's third-party SDK disclosure is marked as disclosed as it is explicitly mentioned in its privacy policy which third parties can get a share of user data while some of them were even mentioned specifically with their name. Application provides in-app data privacy control and therefore that criterion is marked as yes.

MyFitnessPal application on the other hand upon its initial execution forces the creation of an account before any other activity making its features completely inaccessible without that. During the e-mail registration phase users are required to explicitly consent to the processing of sensitive personal data and their cross-border transfer to servers located in the United States. Data protection laws may differ to those in the European Union what makes this transfer a mandatory prerequisite if the user wants to create an account. Despite this rigid requirement, the platform provides an interface through which the user can choose which data can be used for the personalisation and user profiling right after the registration. Those can be set manually or simply fully accepted or rejected. Testing of "deny all" option showed no issues that compromise software performance. Consequently, granular permission control is rated as yes. Furthermore, the dangerous permissions criterion is rated as high due to its extensive integration with critical system layers and external health repositories as well as its use and process of user's biometrical data. Third-party SDK disclosure is marked as disclosed as the external entities were mentioned repeatedly and transparently in privacy policy as well as in application itself. Finally, the platform receives a yes for in-app

data privacy control as it contains a dedicated privacy center which helps users to manage their data processing consents even allowing them to view and restrict access for individual third-party vendors by specific name.

Noom application presents an intrusive user experience upon its first execution as it immediately requests runtime permission to send push notifications before any primary features can be accessed. Following this prompt, the interface provides a lengthy questionnaire as it was the case with BetterHelp but these questions are more related to the user's body weight. These questions as well serve the purpose of extracting behavioral and personal data before account creation. Noom received a high grade for dangerous permissions criterion as can request permissions to access physical activity monitoring, biometric sensors and location data. However, users can block the platform from having these permissions and still use its functionalities normally which consequently resulted with grade yes in granular permission control criterion. Third-party SDK disclosure is marked as disclosed because all of the external entities that can process data gathered by this application are named. In contrast the application fails to provide a universal in-app data privacy control framework. Testing the application on this criterion revealed its complete absence although it provides users with an option to fill out the form within Noom's documentation which serves as an opt-out form. This form appeared to be non-existent in some geographic regions and that happened in this case. Consequently, not all users can opt-out of their data being processed which resulted in a "partial" grade for the last criterion.

7 Conclusion

This study reviews current advances in mobile app development research and assesses the strategies used by developers to protect user data. We use bibliometric analysis, specifically performance analysis and scientific mapping, to uncover new trends and investigate the domain's intellectual structure.

Furthermore, the paper discusses major security threats to developers and users. A qualitative case study examines at BetterHelp, MyFitnessPal, and Noom, three popular Android health applications that handle sensitive medical and personal data, which raises privacy concerns. The findings show that, while these applications preserve fundamental functionality without requiring excessive system rights, gaps in universal in-app privacy settings persist. Ultimately, safeguarding sensitive user data requires a combination of proactive developer responsibility and informed user.

Acknowledgments

This work is supported by the project "HeyAlde - Health Empowerment for You through AI Direct Engagement" co-funded by the European Union from the European Regional Development Fund.

References

- Chin, E., Felt, A. P., & Wagner, D. (2021). Analyzing Inter-Application Communication in Android. *MobiSys 2021 - Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, (pp. 239–252.)
- CNIL. (2025). *Recommendation on mobile applications.*, Published on 8 April 2025, Retrieved from <https://www.cnil.fr/sites/cnil/files/2025-05/recommendation-mobiles-app.pdf>
- Donthu, N., Kumar, S., Mukherjee, D., Pandey, N. and Lim W.M. (2021). How to conduct a bibliometric analysis: An overview and guidelines, *Journal of Business Research*, 133, 285-296.
- EDPB. (2025). *Joint Guidelines on the Interplay between the Digital Markets Act and the General Data Protection Regulation*. Retrieved from https://www.edpb.europa.eu/public-consultations/joint-guidelines-on-the-interplay-between-the-digital-markets-act-and-the_en
- EDPB. (2020). *EU Data Protection Code of Conduct for Cloud Service Providers*. Retrieved from <https://eucoc.cloud/en/>
- ENISA. (2017). *Privacy and data protection in mobile applications A study on the app development ecosystem and the technical implementation of GDPR*. Retrieved from <https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-2-2-4%20GDPR%20Mobile.pdf>
- European Parliament and the Council of the European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L 119, pp. 1–88. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679>
- European Parliament and the Council of the European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), Official Journal of the European Union, L 333, pp. 80–152, Retrieved from <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). Android permissions: User

- attention, comprehension, and behavior. *SOUPS 2012 - Proceedings of the 8th Symposium on Usable Privacy and Security*. <https://doi.org/10.1145/2335356.2335360>
- Grace, M., Zhou, Y., Zhang, Q., Zou, S., & Jiang, X. (2012). RiskRanker: Scalable and accurate zero-day android malware detection. *MobiSys'12 - Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services*, (pp. 281–293). <https://doi.org/10.1145/2307636.2307663>
- Information Commissioner's Office. (2023). *Code of practice for app store operators and app developers (updated)*. Retrieved from <https://www.gov.uk/government/publications/code-of-practice-for-app-store-operators-and-app-developers/code-of-practice-for-app-store-operators-and-app-developers-new-updated-version>
- Marie-Pierre Gagnon, Patrice Ngangue, Julie Payne-Gagnon, M. D. (2016). m-Health adoption by healthcare professionals: a systematic review. *Journal of the American Medical Informatics Association*, 23(1), 212–220.
- Marot, N. (2016). *European Commission_2016_Draft Code of Conduct on privacy for mobile health applications*. 1–23. Retrieved from [file:///134.60.40.17/h-klips\\$!/Austausch/Eva/CitaviAttachments/European Commission_2016_Draft Code of Conduct on privacy for mobile health applications.pdf](file:///134.60.40.17/h-klips$!/Austausch/Eva/CitaviAttachments/European%20Commission_2016_Draft%20Code%20of%20Conduct%20on%20privacy%20for%20mobile%20health%20applications.pdf)
- OWASP. (2026). *OWASP Mobile Top 10 | OWASP Foundation*. Retrieved from <https://owasp.org/www-project-mobile-top-10/>
- Point, C. (2026). *What is a Banking Trojan? - Check Point Software*. Retrieved from <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-trojan/what-is-a-banking-trojan/>
- Raas Cloud. (2026). *50+ Surprising Mobile App Development Statistics 2026*. 2026. Retrieved from <https://raascloud.io/mobile-app-development-statistics/>
- SensorTower. (2026). *State of Mobile 2026 The industry's leading report*. Retrieved from https://sensortower.com/report/state-of-mobile-2026/download?mkt_tok=MzUxLVJXSC0zMTUAAAGiZeg-F7h3yr_dQ4TxMaUIFVv7lBdMX0VAAAtUVObc-pjnMzs7SUBrITuuSpzkch7SR-ZorhTlMsNN3Dd0LyZWX9F_KLFIHwtajL4CBYRF79CBU2I3M
- Statista. (2025.). *Distribution of global mobile malware by type Q2 2025| Statista*. Retrieved from <https://www.statista.com/statistics/653688/distribution-of-mobile-malware-type/>
- Threat, K. (2026). *Trojan-Spy*. Retrieved from <https://threats.kaspersky.com/en/class/Trojan-Spy/>
- World Intellectual Property Organization. (2021). *A Guide to Data Protection in Mobile Applications 2021*. Retrieved from <https://www.wipo.int/export/sites/www/ip-development/en/agenda/pdf/wipo-guide-data-protection-mobile-apps.pdf>
- Xu, Q., Zheng, R., Walid, S., & Han, Z. (2016). Device Fingerprinting in Wireless Networks: Challenges and Opportunities. *IEEE Communications Surveys & Tutorials*.