Evaluating Security and Privacy Features of Quick Response Code Scanners: A Comparative Study

*Ahmad Sahban Rafsanjani[1], Norshaliza Binti Kamaruddin[2], Nilam Nur Amir Sjariff [3], Nurazean Maarop [4], Hazlifah Rusli [5], Nurulhuda Firdaus [6]

[1,2,3,4,5,6]*Faculty of Technology and Informatics Razak, Universiti Teknologi Malaysia*
ahmad_sahban@yahoo.com[1], norshaliza.k@utm.my[2] , nilamnur@utm.my[3], huda@utm.my[4], hazlifah@utm.my[5], nurazean.kl@utm.m[6]

Article history

Received:
20 Sep 2022

Received in revised form:
30 Nov 2022

Accepted:
1 Dec 2022

Published online:
15 Dec 2022

*Corresponding author
ahmad_sahban@yahoo.com

Abstract

Quick Response (QR) codes have become popular in recent years and are extensively utilized in a variety of sectors due to their large capacity, readability speed, and ease of generation and distribution. Besides a broad range of QR code advantages, it attracts the attention of cyberattackers. QR codes may be exploited to distribute harmful information by inserting malicious URLs into QR codes. The security hardening of QR code scanners is the most effective method for detecting and preventing QR code-based attacks. However, the security features of QR code scanners have received little attention in the literature and market. This paper provides a comprehensive evaluation of QR code scanner applications from a security and privacy perspective. We presented the possible attack scenarios on the QR code scanners and reviewed the security mechanisms provided by the scanners. We evaluate secure QR code scanner applications by phishing and malware QR codes. Also, we focus on the potential threats to the privacy of Android QR code scanner applications and assess the permission that is requested during installation. Finally, we have provided guidelines for designing a secure, usable, and privacy-friendly QR code scanner.

Keywords: *QR code scanner, Android security, QR code security, malicious URL, QR code privacy*

1. Introduction

The Quick Response code (QR code) is a known two-dimensional barcode, and it was invented by the Japanese company Denso Wave in 1994 [1]. A QR code has the capability to encode a variety of data types, such as URLs, text, Wi-Fi passwords, vCard, SMS, applications, books, files, etc. [2]. QR codes are extensively utilized in a variety of sectors such as payment, advertising, access control, product identification, and recently for the COVID-19 vaccine and health tracking due to their high data capacity, readability speed, and reliability (compared to 1D barcodes). The widespread adoption of smartphones has resulted in the ability to access QR code information and acceptance among users worldwide. Most modern embedded with smartphones have the capability to scan QR codes by using cameras or by using QR code scanner applications [3].

Besides a broad range of QR code advantages to the users, it also has the capability in attracting the attention of cyberattackers [5]. QR codes may be exploited to distribute harmful information through inserting malicious URLs that look like advertisements, electronic vouchers, electronic surveys, or application download links, etc. Victims are tricked into clicking on such malicious links and unintentionally redirecting to a phishing website or installing malicious applications, resulting in device compromise and loss of sensitive information [6].

Several attack scenarios are possible on the QR code scanner depending on whether it is human or automated, such as phishing, malware propagation, cross-site scripting (XSS), SQL injection, command injection, etc [7, 8]. The attacks that involve human intervention are the focus of this study, which includes phishing and malware propagation. Also, we focus on the potential threats to the privacy of Android QR code scanner applications by facing attacks on the scanner application by requesting unusual permissions from users during installation.

Phishing and malware are among the most popular malicious URL attacks, which occur daily and harm millions of people, and can target various operating systems [9, 10]. A QR phishing attack is a form of phishing attack in which the attacker encodes a malicious URL in a QR code [11,12]. Phishing is the most frequent attack using QR codes in which the victim scans the QR code symbol with their smartphone and is led to a fake website that appears to be legitimate in order to steal sensitive information such as login details and credit card numbers [13,14].

Besides, malicious websites are frequently used by attackers to deliver malware software, and the adoption of QR codes together with malware propagation is a growing concern [15]. In this method, the attacker encodes a malicious URL in a QR code and, once scanned by a QR code scanner, it will direct the victim to a webpage from where they can be driven by a download attack. The attacker can infect the user's systems and cause serious harm through viruses, ransomware, spyware, botnets, Trojan horses, or worms [16].

In this research, we provide a comprehensive study of QR code scanner applications from the perspective of security and privacy. We evaluate secure QR code scanner applications by using the phishing and malware QR codes. Also, we focus on the potential threats to the privacy of Android QR code scanner applications and assess the permission that is requested during installation. Finally, we provide guidelines for designing a secure, usable, and privacy-friendly QR code scanner.

2. Related Work

In this section, we will review the QR code scanner in terms of security and privacy. First, we present the security methods used by QR code scanner applications. Second, we review the standard architectural of privacy-friendly QR code scanner applications with the least privilege permission.

2.1 Security of QR Code Scanners

The normal user has difficulty distinguishing between benign (safe) and malicious (harmful) QR codes due to the fact that QR codes are unreadable by human eyes and can be read only using specific scanning devices. Some QR code scanner applications provide a security method to prevent users from malicious URL threats. However, there is some research in the literature providing security QR code scanner applications. The current QR code scanner applications that offer security are cryptography-based and link security-based security applications [16, 17].

2.1.1 Cryptographic-based

Cryptographic-based methods are utilized in the scanners to encrypt, sign, and control access to QR code content, which provides confidentiality and privacy [5]. Furthermore, digital signatures can accomplish authentication, integrity, and non-repudiation [16]. The size overhead is a major issue while designing these types of scanners, along with issues like selecting an appropriate algorithm, key length, and structure [8].

However, only a limited number of apps support generating and scanning encrypted QR codes. BarSec Droid [18] proposed a comprehensive barcode security scanner by adopting symmetric and asymmetric cryptographic mechanisms and offers barcode authentication, data integrity, access control, and confidentiality [19]. [20] describes the AMP QR Code Scanner anti-malware and phishing detection method, which provides encryption for QR codes by using the AES mechanism.

2.1.2 Link Security-based (URL-based)

URL-based methods are an online protection technique that is provided by the scanner applications, which analyze the URLs encoded in QR codes and prevent users from being redirected to a malicious website for the purposes of phishing and malware attacks [16, 19]. Several methods are utilized for detecting malicious URLs.

The blacklist method is the most preferred approach for QR code scanners [25, 27–32, 37]. URLs that have already been identified as potentially dangerous (phishing, malware) are located in blacklist databases and have gathered over time [21]. It is assumed that a URL is harmful if it appears in the blacklist database and a warning is produced; otherwise, it is benign. This strategy is extremely fast and simple to implement due to the minimal query overhead, and it produces very low false positive errors [11, 22].

The most popular blacklist Application Programming Interface (API) that have been used in QR code scanners are Google Safe Browsing, VirusTotal and

PhishTank. [5] proposes SafeQR, a QR code scanner which is able to detect phishing and malware attacks by invoking the APIs of Google Safe Browsing and PhishTank. [20] points out the AMP QR code scanner, an anti-malware and phishing detection method for Android applications, by calling the VirusTotal API.

Recently, the machine learning detection method has been used by a few QR code scanners [6, 16, 23]. Since big data analytics has become increasingly popular, machine learning techniques that are both generalizable and resistant to real attacks have evolved as the most widely used means of detecting malicious URLs [35]. [6] presents QRFence, a threat-oriented QR malicious link detection framework, based on a novel machine learning model which integrates multiple classification algorithms. [23] proposes QRphish, an automated QR code phishing detection approach based on a Bayes classifier machine learning model. [16] describes BarAI, secure real-time artificial intelligence system against malicious QR Code links.

2.2 Privacy-friendly Scanners

The safety of QR code scanner applications is a major concern for QR code security [12, 21]. There are several potential threats to the privacy of Android devices, but the most significant is the application's request for excessive permission [19]. There is always the possibility that an attacker would discover a vulnerability in a QR code scanner, and because many scanners seek full permission to access the user's smartphone resources during the installation process, an attacker may gain access control over the entire smartphone and acquire entry to the user's sensitive data [6].

Developers request a variety of permissions from the end user’s smartphone, but they may be unaware of the risks associated with obtaining these permissions. According to [16, 19], privacy-friendly QR code scanner applications need standard architectural choices for developers to build applications with the least privilege permission. The necessary permissions that should be requested from applications are:

- Camera: takes pictures and videos.
- Network: gives full network access and views network connections.
- Wi-Fi: view Wi-Fi connections.

However, some of these scanner applications request unusual permissions, such as changing or erasing the contents of the user's SD card, location, microphone, Bluetooth, telephone access for the purpose of directly calling phone numbers, SMS, and drawing over the other apps to modify system settings, etc.

3. Performance Evaluation

In this section, we evaluate a comprehensive systematic review of QR code scanners and evaluate several applications from the security and privacy perspective.

3.1 Evaluation Security Features of QR Code Scanners

In this section, we present a comprehensive systematic review of QR code scanner applications on Android and evaluate several scanner applications from a security perspective. These apps were selected randomly based on previous studies, popularity, and security features. Table 1 shows the details of the applications that were reviewed. The items that are considered are version, number of downloads, rate, and security features. As can be seen in this table, several scanners that have been downloaded millions of times lack security features to protect users from threats [24, 26].

Table 1. Specifics of evaluated QR code scanners

App Developer	Version	Size (MB)	Downloads	Rate	Security Features
[24]	2.2.12	5.2	100M+	4.7	N/A
[25]	2.7.1-L	2.72	100M+	4.6	URL Checking
[26]	2.2.8.GP	6.26	10M+	4.8	N/A
[27]	1.1.0	8.7	500K+	4.7	URL Checking
[28]	1.0.3.14d044e2	3.2	10K+	2.9	URL Checking
[29]	1.8.4.260	18.2	5M+	4.5	URL Checking
[30]	7.0.6	10.1	50M+	4.3	URL Checking & Encryption
[31]	1.1.0	1.9	100K	4.3	URL Checking
[32]	9.6.3434	21	1M+	4.3	URL Checking
[33]	1.3	5.85	100K+	4.3	N/A
[34]	1.0.18	10	100K+	4.5	N/A
[35]	1.0.3.18	2.16	100+	4.3	N/A
[36]	1.0.2	21.1	10+	-	N/A
[18]	1.3	2.7	-	-	URL Checking & Encryption
[37]	1.0.0	10.63	10+	-	URL Checking

[19, 38] present the criteria for developing a secure and usable QR code scanner. Table 2 illustrates the components that were analyzed for secure QR code scanners. These components are: check URL (security feature), display URL, get full URL (redirect), directly open URL, URL checking method, and detection model.

Table 2. Evaluating secure QR code scanner

APP Developer	Check URL	Display URL	Get Full URL	Direct Open	URL Checking Methods	Detecting Model
[25]	Yes	Yes	No	No	Google Safe Browsing	Blacklist
[27]	Yes	Yes	No	If safe Yes unless No	Trend Micro security	Blacklist
[28]	Yes	Yes	Yes	No	G Data security	Blacklist
[29]	Yes	No	No	Yes	Kaspersky Virus desk	Blacklist

[30]	Yes	Yes	No	No	Google Safe Browsing	Blacklist
[31]	Yes	No	No	No	Cheetah Mobile browser	Blacklist
[32]	Yes	Yes	No	No	Intelligence Sophos Lab security	Blacklist
[18]	Yes	Yes	Yes	No	Google Safe Browsing, PhishTank	Blacklist and heuristic method
[37]	Yes	Yes	No	No	Lionic malicious web cloud database.	Blacklist

As seen in this table, the majority of secure QR code scanners do not meet baseline security requirements. [25, 27, 29-32, 37]are unable to redirect a URL and obtain the full URL, even though some of them [27, 29] immediately access the website without user permission. Furthermore, the major detection model utilized in these applications is the blacklist model, and it is hard to discover scanners that employ alternative detection methods [18].

The malicious URLs have been generated to analyze the security level of QR code scanners. The Zoo [39] and Zphisher [40] toolkits have been used to generate malicious URLs for phishing and malware propagation toolkits on GitHub. The Zoo is a very popular malware repository for analysis and enables researchers who are interested to evaluate around 350 live malware projects. The Android malware applications Dendroid and Android Spy iBanking in APK format are employed to assess the security of QR code scanners. Also, Zphisher provides multiple updated phishing tools and allows users to perform phishing attacks on several sites and social media, such as Facebook, Twitter, PayPal, Instagram, Netflix, and many more. In this study, PayPal was selected for a phishing attack. Finally, the most well-known URL shortening website, Bitly [41], was utilized to generate short URLs to evaluate the usability of existing secure scanners. The main reason for using short URLs is that the most secure QR code scanners are not able to detect URL redirection.

Table 3 demonstrates the evaluation of secure QR code scanners. There are seven malware and phishing QR codes utilizing to evaluate the malicious URL detection effectiveness of these scanners. These QR codes are Dendroid embedded in a QR code, Dendroid QR code shorten using Bitly, iBanking embedded in a QR code, iBanking QR code shorten using Bitly, phishing PayPal QR code using the original Zphisher tunnel, PayPal QR code shorten using Bitly, and the PayPal link embedded in a normal QR code generator.

Table 3. Evaluate secure QR code scanners using nine malware and phishing QR codes.

APP Developer	Dendroid QR code	Dendroid Bitly QR code	iBanking QR code	iBanking Bitly QR code	PayPal original tunnel QR code	PayPal Bitly QR code	PayPal QR code generator
[25]	No	No	No	No	No	No	No
[27]	Un	No	Un	No	No	No	No
[28]	No	No	No	No	Sus	Sus	Sus
[29]	No	No	No	No	No	No	No
[30]	No	No	No	No	No	No	No
[31]	No	No	No	No	No	No	No
[32]	No	No	No	No	No	No	No
[18]	Yes	No	Yes	No	Yes	Yes	No
[37]	No	No	No	No	No	No	No

The outcome reveals that BarSec Droid [18] is capable of detecting some harmful websites, and G-DATA [28] is suspicious about phishing attacks, while others lack the ability to detect malicious URLs. The issue with some scanners to evaluate is that they feature a suspicious-URL option that might make it difficult to distinguish between malicious and safe links.

Due to the fact that QR codes are not visible to human eyes and require scanners to read the information, users usually trust secure QR code scanners to protect them from potential harm. However, they are not able to detect the malicious URLs because the method they are using is mostly the blacklist method, which is not exhaustive and cannot identify newly created malicious URLs. Furthermore, some of these secure scanners are developed by famous internet security service providers such as Trend-Micro, Kaspersky, Sophos, and Falcon-Security-Lab and offer secure QR code scanner apps.

3.2 Permission and Privacy Evaluation

In this part, we provide an overview of Android QR code scanners and assess all the examined applications based on the permissions they require during installation. Table 4 shows the requested access from the applications such as accessing the camera, storage, location and etc.

Table 4. Requested permission from applications during installation.

APP Developer	Cam	Stg	Loc	Cont	wi-fi	Files	Ph	DevID	DevHis	Cal	Net	Oth
[24]	✔	✔	✔		✔	✔					✔	✔
[25]	✔	✔	✔	✔	✔						✔	✔
[26]	✔	✔			✔						✔	✔
[27]	✔	✔		✔	✔						✔	✔
[28]	✔	✔	✔		✔						✔	✔
[29]	✔	✔			✔					✔	✔	✔
[30]	✔	✔	✔	✔	✔						✔	✔
[31]	✔	✔		✔	✔		✔				✔	✔
[32]	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔

[33]	✔	✔	✔		✔		✔				✔	✔
[34]	✔	✔			✔		✔	✔	✔		✔	✔
[35]	✔	✔			✔						✔	✔
[36]	✔	✔	✔	✔	✔		✔			✔	✔	✔
[18]	✔	✔			✔						✔	
[37]	✔	✔		✔	✔						✔	✔

According to [16, 19], save privacy, QR code scanner applications with the least privilege permission must only request access to the camera, Wi-Fi, and network. However, some of these applications request unusual permission during installation. Most applications request access to storage to read, modify, or delete the contents. [27] request for microphone access; [30] asking for Bluetooth permission; [24, 25, 28, 30, 31, 32, 36] requesting access to the location. [31] asks for uncommon permissions to read contacts, call, SMS, and draw over the other apps' modified system settings. [32] requests extremely abnormal access to draw other apps, control near-field communication, retrieve and run other apps, and read phone status and identity. [33] request access to the telephone for the purpose of directly calling phone numbers. [29, 36] requesting permission to access the calendar.

4 Design Recommendation

We suggest the following criteria for developing secure, usable, and privacy-friendly QR code scanner applications based on our analysis of the current scanners, the limitations and drawbacks identified, and the recommendations in another researches [19, 20, 22].

4.1 QR code Scanner Security

The secure QR code scanner should be able to detect malicious URLs. Here we have two suggestions for designing a secure QR code scanner. First, we suggest designing a malicious URL detection model for secure QR code scanners, which can identify URLs in real time with a high level of accuracy. For this purpose, feature classification is suggested. It may extract a variety of information about a URL utilizing blacklist, lexical, host-based, and content-based features. This information might be used to predict the behavior of malicious URLs. Additionally, these features may be classified using supervised machine learning techniques, such as Random Forest or Support Vector Machines, or, more recently, researchers have focused on detecting harmful URLs using deep learning.

The second recommendation is to examine URLs for redirection. The scanner may examine the URL for redirection and, if identified, automatically redirect it to the original URL. The specific purpose is to redirect URLs to the original website in order to evaluate features if a short URL is used. Also, it suggests displaying both websites to the users, which helps to make users aware of innocent looking short URLs so that later they can distinguish between legitimate and malicious URLs.

4.2 QR Code Scanner Privacy

Privacy-friendly QR code scanner applications should take least privilege permission. The necessary permissions that should be requested from applications are:

- Camera: takes pictures and videos;
- Network: gives full network access and views network connections.
- Wi-Fi: view Wi-Fi connections;

Furthermore, additional permission may be requested from the user according to the scanner features. These acceptable permissions may be getting access to storage to read QR code images from the phone, getting access to the flashlight for situations that need more light for scanning, and accessing the history for the scanned images. The most important criteria will be that all of these permissions should not be taken during installation and only added in the case that a user needs to use the features.

4.3 QR Code Scanner Usability

Features that might be added to QR code scanners to improve their usability are listed below.

- **Warnings:** Display a warning to the user regarding the maliciousness of the URL and make the user aware if open it.
- **URL status:** shows to the user the status of a URL, whether it is malicious or benign (do not add a suspicious option).
- **Display URLs:** Display original and redirected (if any) URLs.
- **Simple interface:** Provide a simple interface for normal users.
- **Response time:** The detection result must be returned in less than 5 seconds.
- **Application security:** The scanner should provide a secure QR code application.
- **Special features:** The special features may be provided by the application which make it more usable, such as the ability to scan images using both the front and rear cameras, enable the flashlight, and access a history of scanned QR codes.

5. Conclusion

This paper presents a comprehensive evaluation of QR code scanner applications from a security and privacy perspective. We present the possible attack scenarios on the QR code scanners and reviewed the security mechanisms provided by the scanners. Also, we evaluate secure QR code scanner applications by some

phishing and malware QR codes. Furthermore, we focus on the potential threats to the privacy of Android QR code scanner applications and assess the permission that is requested during installation. Finally, we have provided guidelines for designing secure, usable, and privacy-friendly applications. In future work, we plan to develop a secure QR code scanner, QsecR, a malicious URL detection model that can detect new malicious URLs in real time with a high level of accuracy. This application provides an effective feature classification for identifying malicious URLs.

References

[1]. Denso Wave, "Quick Response Code (QR code)," https://www.denso-wave.com/en/, 2022.
[2]. Rafsanjani, A. S (2018). Comparison Cover Image of Digital Watermarking Based on Discrete Cosine Transform by Using Quick Response Code. 1st International Conference on Emerging Trends in Engineering, Technologies and Social Sciences (ICETS-2018).
[3]. Chou, G. J., & Wang, R. Z. (2020). The nested QR code. IEEE Signal Processing Letters, 27, 1230-1234.
[4]. DAVID CURRY, Android Statistics (2022). https://www.businessofapps.com/data/android-statistics/#:~:text=Android%20has%2038%20percent%20market,had%2045%20percent%20market%20share,%202022.
[5]. Yao, H., & Shin, D. (2013, May). Towards preventing QR code-based attacks on android phone using security warnings. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security (pp. 341-346).
[6]. Song, J., Gao, K., Shen, X., Qi, X., Liu, R., & Choo, K. K. R. (2018). QRFence: A flexible and scalable QR link security detection framework for Android devices. Future Generation Computer Systems, 88, 663-674.
[7]. Averin, A., & Zyulyarkina, N. (2020, November). Malicious Qr-Code Threats and Vulnerability of Blockchain. In 2020 Global Smart Industry Conference (GloSIC) (pp. 82-86). IEEE.
[8]. Focardi, R., Luccio, F. L., & Wahsheh, H. A. (2018). Security threats and solutions for two-dimensional barcodes: a comparative study. In Computer and network security essentials (pp. 207-219). Springer, Cham.
[9]. Patil, D., & Patil, J. (2018). Feature-based malicious url and attack type detection using multi-class classification. The ISC International Journal of Information Security, 10(2), 141-162.
[10]. Sahoo, D., Liu, C., & Hoi, S. C. (2017). Malicious URL detection using machine learning: A survey. arXiv preprint arXiv:1701.07179.
[11]. Vidas, T., Owusu, E., Wang, S., Zeng, C., Cranor, L. F., & Christin, N. (2013, April). QRishing: The susceptibility of smartphone users to QR code phishing attacks. In International Conference on Financial Cryptography and Data Security (pp. 52-69). Springer, Berlin, Heidelberg.
[12]. Kusyanti, A., & Arifin, A. (2017). QRishing: a user perspective. International Journal of Advanced Computer Science and Applications, 8(10).
[13]. Yong, K. S., Chiew, K. L., & Tan, C. L. (2019, June). A survey of the QR code phishing: the current attacks and countermeasures. In 2019 7th International Conference on Smart Computing & Communications (ICSCC) (pp. 1-5). IEEE.
[14]. Mavroeidis, V., & Nicho, M. (2017, August). Quick response code secure: a cryptographically secure anti-phishing tool for QR code attacks. In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (pp. 313-324). Springer, Cham.
[15]. Sharma, V. (2012). A study of malicious QR codes. International Journal of Computational Intelligence and Information Security, 3(5), 21-26.
[16]. Al-Zahrani, M. S., Wahsheh, H. A., & Alsaade, F. W. (2021). Secure Real-Time Artificial Intelligence System against Malicious QR Code Links. Security and Communication Networks, 2021.
[17]. Wahsheh, H. A., & Luccio, F. L. (2019, February). Evaluating Security, Privacy and Usability Features of QR Code Readers. In ICISSP (pp. 266-273).
[18]. Heider Wahsheh, "BarSec Droid." 2018. https://m.apkpure.com/barsec-droid/barcode_security.heider.apk
[19]. Wahsheh, H. A., & Luccio, F. L. (2020). Security and privacy of QR code applications: a comprehensive study, general guidelines and solutions. Information, 11(4), 217.
[20]. Hemavathi, P., Hegde, N., Bharti, R, Sur, R., & Priyanka S, (2018). Anti-Malware Phishing QR Scanner. International Journal of Innovative Science and Research Technology. Volume 3, Issue 5.
[21]. Latif, K. A., Sugiantoro, B., & Prayudi, Y. (2019). Anti-Qrishing Real-Time Technique on the QR Code Using the Address Bar-Based and Domain-Based Approach on Smartphone. International Journal of Cyber-Security and Digital Forensics, 8(2), 134-144.
[22]. Krombholz, K., Frühwirt, P., Rieder, T., Kapsalis, I., Ullrich, J., & Weippl, E. (2015, August). QR Code Security--How Secure and Usable Apps Can Protect Users Against Malicious QR Codes. In 2015 10th International Conference on Availability, Reliability and Security (pp. 230-237). IEEE.
[23]. Alnajjar, A. Y., Anbar, M., Manickam, S., Elejla, O., & El-Taj, H. (2016). QRphish: An Automated QR Code Phishing Detection Approach. Journal Of Engineering and Applied Sciences, 11(3), 553-560.
[24]. Gamma-Play, QR & Barcode Scanner. (2022). https://play.google.com/store/apps/details?id=com.gamma.scan
[25]. TeaCapps, QR & Barcode Reader. (2022). https://play.google.com/store/apps/details?id=com.teacapps.barcodescanner.
[26]. InShot-Inc., Free QR Scanner - Barcode Scanner, QR Code Reader. (2022). https://play.google.com/store/apps/details?id=qrscanner.barcodescanner.barcodereader.qrcodereader.
[27]. Trend-Micro, QR Scanner - Free, Safe QR Code Reader, Zero Ads. (2022). https://play.google.com/store/apps/details?id=com.trendmicro.qrscan.
[28]. G DATA QR Code Scanner. (2022). https://www.gdatasoftware.com.
[29]. Kaspersky, QR Code Reader and Scanner: App for Android. (2022). https://play.google.com/store/apps/details?id=com.kaspersky.qrscanner&referrer=af_tranid%3DFvrg4d22ypPkZQbxXQK

AVQ%26pid%3Dacq%26c%3Dacq-freekasp-COM-QRS-Android%26af_web_id%3Dae14f451-2652-4bf8-b3e3-394a0713e12c-c, 2021.
[30]. DroidLa, QR Droid. (2022) https://play.google.com/store/apps/details?id=la.droid.qr.
[31]. Cheetah-Mobile, Cheetah Mobile QR code & Bar Code Scanner. (2022). https://cm-qrcode.en.aptoide.com/app.
[32]. Sophos-Limited, Sophos Intercept X for Mobile. (2022).
[33]. Falcon-Security-Lab, QR Code Scanner & Barcode Reader. (2022). https://play.google.com/store/apps/details?id=com.falcon.barcodescanner.
[34]. Easy-TechMobile, Safe Scanner-best QR code reader, Barcode scanner. (2022). https://play.google.com/store/apps/details?id=app.safe.barcode.qrcode.scanner, 2021.
[35]. Alexandr Unger, SafeQR. (2022). https://play.google.com/store/apps/details?id=biz.ungerware.safeqr&hl=en&gl=US.
[36]. Samuel Bifalco, SafeQR . (2022)
[37]. Lionic Secure QR Code Scanner. (2022). https://play.google.com/store/apps/details?id=com.lionic.scanner.qrcode, 2022.
[38]. Dudheria, R. (2017, October). Evaluating features and effectiveness of secure QR code scanners. In 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) (pp. 40-49). IEEE.
[39]. Ytisf, TheZoo - A Live Malware Repository. (2014) https://github.com/ytisf/theZoo.
[40]. Htr-tech, Zphisher. (2022). https://github.com/htr-tech/zphisher.
[41]. Bitly, (2022). https://bitly.com/.