v. 5, n. 1, 2025

Journal of
Engineering
Research

Acceptance date: 08/01/2025

DETECTION AND CONTAINMENT OF QR CODE ATTACKS (MEDUSA; QRISHING/ QUISHING) USING MALWARE IN MOBILE APPLICATIONS IN MEXICO

Juan Jesús Ruiz-Lagunas
Is a tenured professor at the Tecnológico Nacional de México, Morelia campus, Systems and Computing Department
ORCID: 0000-0002-1101-0584

Anastacio Antolino Hernández
Is a tenured professor at the Tecnológico Nacional de México, Morelia campus, Systems and Computing Department
ORCID: 0000-0001-6150-2934

Heberto Ferreira-Medina
Telecommunications manager at the Instituto de Investigaciones en Ecosistemas y Sustentabilidad at UNAM, as well as a tenured professor at the Tecnológico Nacional de México, Morelia campus, Systems and Computing Department
ORCID: 0000-0003-0150-2355

Miguel Espejel Cruz
Telecommunications manager at the Instituto de Radioastronomía y Astrofísica at UNAM Morelia, as well as a tenured professor at the Tecnológico Nacional de México, campus Morelia, Systems and Computing Department
https://www.irya.unam.mx/web/es/gente/tecnicos-academicos/m-espejel

DOI https://doi.org/10.22533/at.ed.317512507012

Guadalupe Ramos Díaz
Is a tenured professor at the Tecnológico Nacional de México, Morelia campus, systems and computing department
ORCID: 0000-0002-7281-7461

Abstract: The use of QR codes (Quick Response) in all areas of technology worldwide is booming, due to their ease of reading and access to computer resources or financial assets, this has repercussions on deception and fraud. to the users and companies that trust them. In theory and practice the codes are safe, but excessive use can lead to deception and threats that cause the theft of personal data and financial fraud. "Qrishing" frauds (a technique that aims to deceive victims by impersonating web pages) are growing at an alarming rate, generating million-dollar losses. This type of fraud, which redirects users to malicious sites by simply scanning a code, or which can also download and install malware on the devices that read it, generates million-dollar losses for companies, governments, and users. This research work proposes an alternative solution to the validation, verification, and detection of malicious software in QR codes, by characterizing the most common attacks (such as the Medusa attack; QRishing/Quishing), based on the consultation and analysis of a mobile application that helps detect malware (malicious software) or links from fraudulent sites, in order to warn and prevent the user from using them.

Keywords: QR, Malware, QRhising, Medusa Attack, Mobil App

INTRODUCTION

Information security (IS) aims to protect data in computer systems in terms of access and use. IS aims to certainty, which is understood as the state of the system or information that is available and can be consulted, and is free of danger, damage, or risk of being used. At the same time, it is also considered as the set of preventive and reactive measures of organizations and those technological systems that allow the safeguarding and protection of information, seeking to keep its confidentiality, availability, and integrity (ISO, 2022). Therefore, having the implementation of good practices, following recommendations, using security policies, methodologies, and rules, among others, guarantees the benefit of using information without errors, to obtain the best result and achieve success in companies.

The advancement of technology is known with its accelerated delivery of products, especially that which focuses on the retail market, without guaranteeing basic security for the information handled and/or shared when using them. This possible disadvantage, combined with the lack of knowledge of good practices, as well as the development of software for secure applications, and the activity of cybercrime (hackers), are one of the most important problems that Mexico faces in the post-pandemic of the COVID-19 virus. 19, and in the digital world.

With the current use, dependence and increase in the number of mobile devices and users that use QR codes, the question we ask ourselves is: do these codes have security features or measures?

A code of this type uses a two-dimensional barcode that was designed to be read by robots that tracked items produced in a factory of the Japanese company Denso-Wave, a subsidiary of Toyota (Vall, 2023). A QR code takes up much less space than a standard barcode, its use has spread across the board. Modern smartphones can easily read these codes, as all that is needed is a camera and light software. Some applications, such as banking ones, have built-in software for reading these codes to make it easier for users to make online payments. In other cases, the codes are also used as part of the registration or login procedure.

As the demand and use of QR codes increases, many users are still skeptical about the security features they may have. This mistruth has been fed with the increasing number of frauds and financial deception cases, along with its popularity. It should be remembered that, with the post-pandemic demands of trying to avoid physical contact, these codes were and remain an alternative solution to this need, but as these codes became widespread, new threats to safety began (Vall, 2023).

In theory and practice the codes are safe, but today the threats that their use can be alarming. It is because of this that "Qrishing" frauds (manipulation technique with QR codes with the aim of deceiving victims by impersonating Web pages) take advantage of its popularity. This type of digital fraud redirects users to malicious sites by simply scanning a code, or it can also download malware; This cybercrime practice is generating million--dollar losses. The Qrishing technique has appeared as one of the most dangerous variants of phishing. Cybercriminals take advantage of trust to carry out attacks that compromise personal and banking data. Consequently, an 81% increase in this type of attacks has been recorded in Mexico (90 Grados, 2024).

There are two types of QR codes that can be generated; 1) static, which are created very easily using free software, standing for a minor threat since they cannot be edited and 2) dynamic, which allow you to create and edit your content and which could pose a threat to users. by allowing modification (Vall, 2023). Being so easy to use means that users, when scanning them in common sites such as financial institutions, restaurants, convenience or department stores, can access unauthorized or fraudulent sites without realizing the risk, thus becoming victims of cybercriminals. Due to this situation, it is advisable to constantly verify the origin of the codes and use the preview of the URL (link) or site, before opening it or sharing personal and/or banking information. One form of prevention is to avoid reading them in public places where there is no security control. It is important to mention that despite the constant dissemination of the risks inherent in the use of QR codes, they are increasingly popular.

LITERATURE REVIEW

According to Huidobro (2009) “A QR code is a system for storing information in a matrix of points that can be represented in print or on a screen and can be interpreted by any device capable of capturing images or with the appropriate reader.” These codes are important due to their high capacity to store information, as well as their accessibility when entering any type of data. They store up to 3KB of information in a horizontally and vertically fashion (Nathaly Castro Acuña, 2019). Due to these characteristics, they are used to carrying out distinct types of transactions and queries. According to Xing Han (2023) with the use of smartphones today we can use these codes both online and offline, which is why it is important due to its versatility of use, currently being a great alternative for companies of all the industries. In a survey carried out by the company Statista (2023), it was found that the most frequent applications for using QR codes in Mexico focus mostly on mobile internet users, where about 64% mentioned using it to see the characteristics of a product. Likewise, other frequent uses were to make purchases and make payments, with 33.5% and 32.8%, respectively, as shown in Fig. 1.

As a result of the earlier survey and the information from Ortega (2022), a list of uses and application opportunities in Mexico for this technology is described:

- In conference rooms and hotels: plain text for welcome messages.
- For advertising: commercial data.
- In security: authentication for online accounts or access codes.
- In restaurants: menus, offers and/or promotions.
- At airports: information about flights or discounts.
- In entertainment: cinema, theater, or related shows.
- In industry: in all areas of technology.
- In financial processes: receiving and making payments, among others.

A series of attack techniques on QR codes are also mentioned, as described below:

Phishing

It is an impersonation technique and is the most used resource (one of the most dangerous) by cybercriminals. They use a combination of social engineering and technical attack methods known as exploits. According to Benavides (2020), phishing attacks consist of a five-stage life cycle, which is shown in Fig. 2.

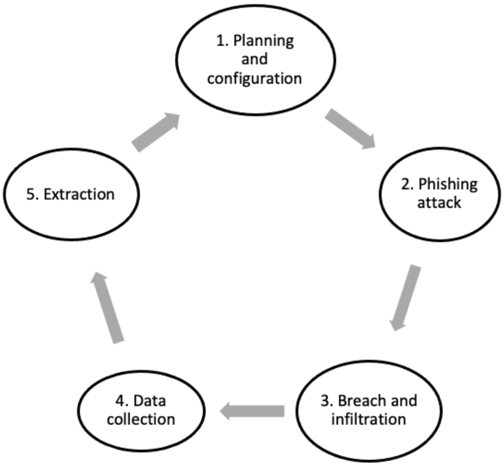


Fig. 2. Phishing attack method described in Benavides (2020).

The phases of phishing are described below:

1. Planning and configuration: the main goal is to extract essential details about the victim and the network, for which traffic analysis can be done

2. Phishing attack: The attackers send the information to the victim requesting confidential information.

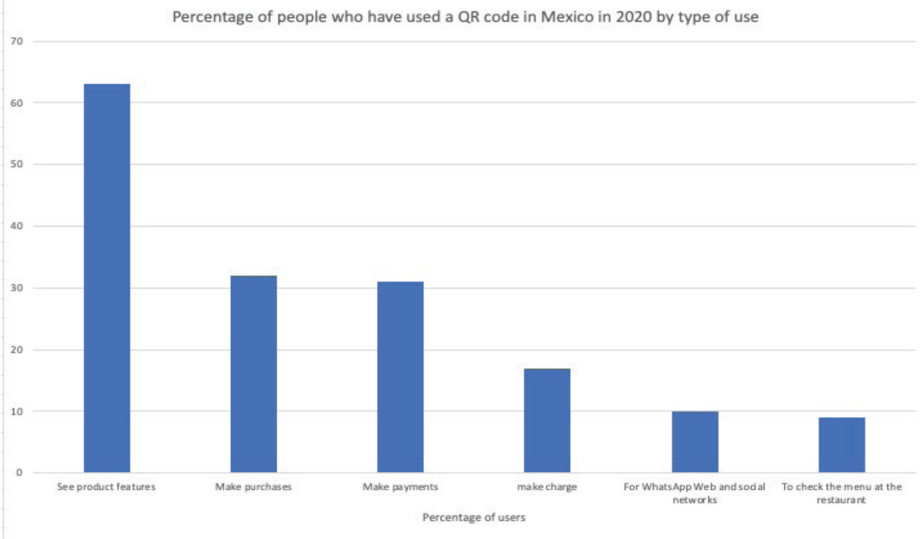


Fig. 1. Use of QR codes in Mexico based in report from Statista (2023).

3. Breach and infiltration: This happens when the victim clicks on the malicious link, leading to the theft of information and the gateway for malware.

4. Data collection: Attackers can range from accessing the user's confidential data to performing denial of service attacks, depending on the severity of the situation.

5. Extraction: attackers tend to drop evidence of fake accounts once their mission has been completed.

QRishing

Also known as QR phishing, according to (Cloudflare, 2020) "…is a cybersecurity threat in which attackers use these codes to redirect victims to malicious websites or induce them to download harmful content." This type of attack aims to steal information ranging from passwords, financial data and/or personal identification information, so, for attackers, introducing the ransomware attack (kidnapping through information encryption) within These codes are simple and extremely useful because they usually bypass conventional security defenses.

Cybercriminals are focusing on attacking smart mobile devices (smartphones) due to poor security, not having effective antivirus systems or firewalls due to the energy expenditure they are. Redirection to infected links ranges from phishing attacks also known as QRLJacking or session hijacking. This consists of downloading malware or injecting malicious code into the destination URL; It is characterized by the download of malicious software designed to exploit the vulnerabilities of the target device, as well as its known vulnerabilities (Bardají, 2022). There are three threats of this type according to itdigitalsecurity (2023), which are mentioned below:

1. QRishing: QR and phishing consists of the design of false codes that redirect to fraudulent websites. that request sensitive information from the user and then violate them.

2. Reverse QR: It is a technique used to redirect users to malicious or fraudulent websites instead of the legitimate page. This is achieved by changing the link associated with the original QR code, which can result in the download of malware, theft of personal or financial information, or even unauthorized access to the reading device.

3. QRLjacking: Technique used to hijack access to services that allow the choice to log in to sites using a QR code, as can occur in social networking applications, allowing you to obtain and view all kinds of sensitive or confidential information.

METHODOLOGY

In this work, a documentary and exploratory research approach is used, where the experiences of related projects consulted in the literature and in methodologies described in projects oriented to security in QR codes are considered. Different methods are observed for impersonation and attacks on mobile systems using different techniques, which include jellyfish-type attacks. Below we mention the most used ones:

- Phishing or impersonation is the most widely used form of attack and one of the most effective, it is a combination of social engineering and exploits. According to Benavides (2020), phishing attacks are classified as: 1) according to the service and 2) according to the modus operandi, e.g. and. "Man in the middle."
- As mentioned above, another attack method is QRishing, which is a redirection to infected links, through phishing or QRLJacking (URL links in QR) or session hijacking (Bardají, 2022).
- Another widely used method is replacing legitimate QR codes with fake ones; this is physically changing the authentic code with fraudulent information.

There are detection and prevention methods that are based on the execution of guardian software, like an antivirus, that can detect the jellyfish attack using different techniques, these are:

- Use of a Blacklist (previously detected malicious QR codes).
- Use of Machine Learning or Deep Learning methods to detect anomalous behavior of the information contained in the code.
- Use of antivirus software (sandbox) as a containment method, based on tracks.
- Use of "Sniffers" analysis tools that can detect anomalous network traffic.
- Use of detection systems based on the information contained in the target website (use of malicious document detection systems).

In recent studies by Kim, D. et al. (2024), several techniques are recognized to violate the access key registration process through the FIDO (Universal Authentication Specification, UAF) client-server method, using an authentication protocol (known as CTAP) in QR codes. As shown in Fig. 3.

The attack method on this protocol is session replication by disconnecting the client's wireless network, as shown in Fig. 4.

The main vulnerability in CTAP logging through code scanning is the browser's ability to connect to multiple authenticators at once. This attack can be stopped by blocking multiple sessions at the browser level.

In this project, a detection method is used based on a blacklist of previously detected malicious QRs (blacklist) and a mobile application that scans and detects malicious code in the destination URL. This method helps the user in making the decision to use the QR or not. Fig. 5 shows the process used as the proposed solution method.

Phases of the method used to detect malicious QRs by the mobile App (WebApp):

1. The attacker changes the original QR code, and impersonates it with a fake one, to send it or wait for the victim to scan it.

2. When the victim reads said code, he or she may be directed to a fraudulent site to steal personal data or be infected by malicious code.

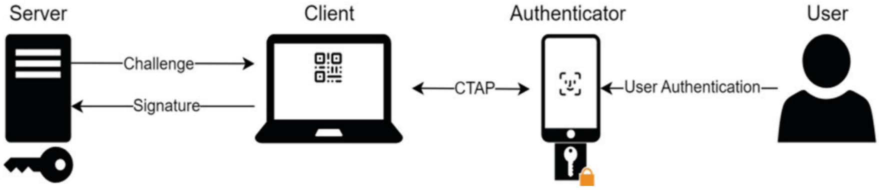


Fig. 3 FIDO CTAP authentication method (Kim, D. et al., 2024).

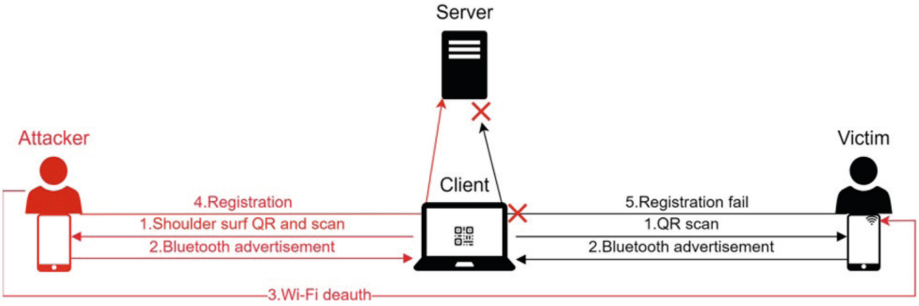


Fig. 4. Session replication attack (Kim, D. et al., 2024).

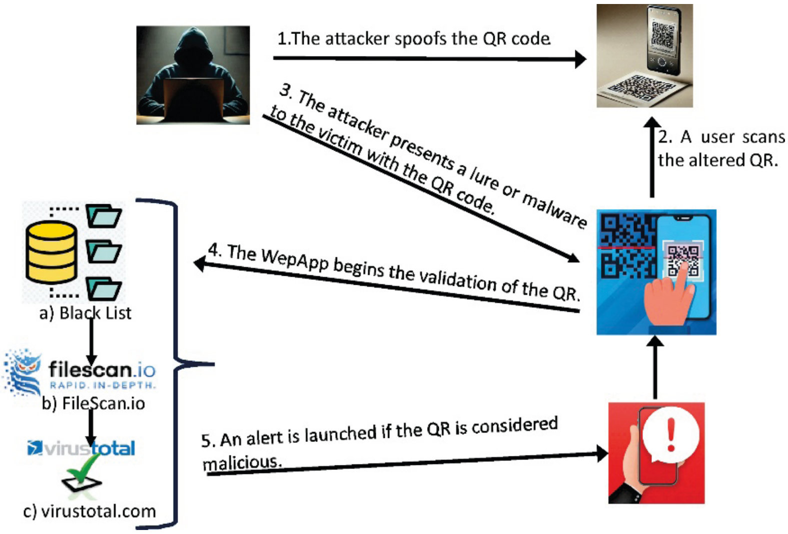
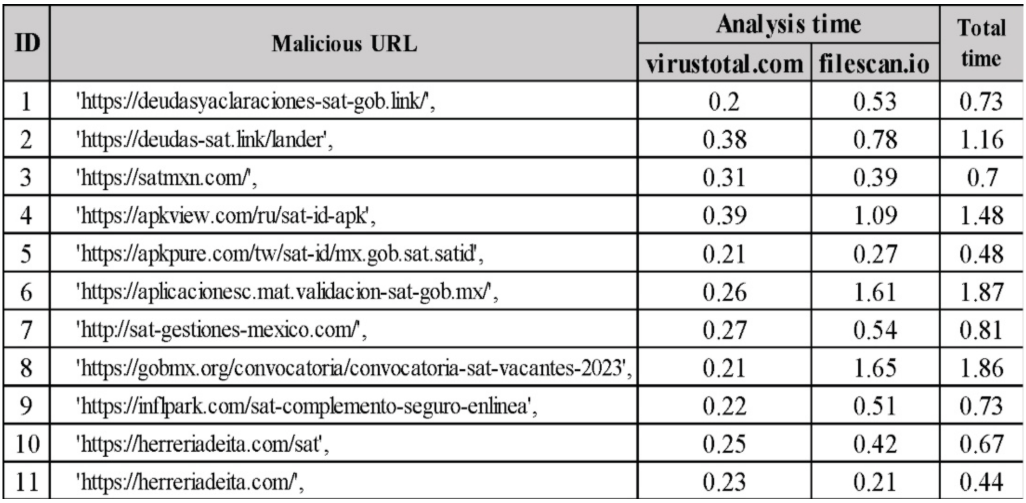

1.The attacker spoofs the QR code
2. A user scans the altered QR.
3. The attacker presents a lure or malware to the victim with the QR code.
4. The WepApp begins the validation of the QR.
5. An alert is launched if the QR is considered malicious.
a) Black List
filescan.io
RAPID. IN-DEPTH.
b) FileScan.io
virustotal
c) virustotal.com

Fig 5. Detection method for compromised QR codes based on a blackList.



ID	Malicious URL	Analysis time		Total time
		virustotal.com	filescan.io	
1	'https://deudasyaclaraciones-sat-gob.link/',	0.2	0.53	0.73
2	'https://deudas-sat.link/lander',	0.38	0.78	1.16
3	'https://satmxn.com/',	0.31	0.39	0.7
4	'https://apkview.com/ru/sat-id-apk',	0.39	1.09	1.48
5	'https://apkpure.com/tw/sat-id/mx.gob.sat.satid',	0.21	0.27	0.48
6	'https://aplicacionesc.mat.validacion-sat-gob.mx/',	0.26	1.61	1.87
7	'http://sat-gestiones-mexico.com/',	0.27	0.54	0.81
8	'https://gobmx.org/convocatoria/convocatoria-sat-vacantes-2023',	0.21	1.65	1.86
9	'https://inflpark.com/sat-complemento-seguro-enlinea',	0.22	0.51	0.73
10	'https://herreriadeita.com/sat',	0.25	0.42	0.67
11	'https://herreriadeita.com/',	0.23	0.21	0.44

Table 1. Cumulative response times for virustotal.com and filescan.io in seconds

3. The attacker waits for the user to become a victim of deception to obtain confidential or financial data.

4. The WebApp checks the code against a blackList on the Local Web Server and/ or online antivirus systems, to decide if it is malware.

5. If the code is detected as malicious, the blackList on the Web Server is updated and a warning is issued to the user that the code is dangerous, and it is recommended not to access it.

RESULTS

The use of a blacklist of Web pages or email addresses, which have been previously reported for fraudulent behavior or for sending email considered unwanted advertising, are solutions widely used in projects such as urlscan.io or filescan.io (INCIBE, 2023). However, it requires a maintenance and support system to avoid false positives. In this work, a website was developed that requires the intervention of an administrator to keep the blacklist. An improvement to this proposed solution is to implement automatic systems to add or delete elements using Web scraping techniques (search for lists on the Internet), or ML techniques that help learn malicious URLs and their possible content (exploration of documents on the target Web) for the update, which would observe a significant improvement.

In this project, a blacklist of phishing Web pages was created as well as malicious URLs obtained through QR code scans, taking this information to control access to fraudulent sites in Latin America. It is important to mention that this list has data that meets characteristics that were added through the following steps:

1. Spam: If the attack is detected on an anti-Spam server based on a Black-List, this address is added to the local Blacklist, to begin blocking emails with said URLs contained in them.

2. Antivirus verification: Antiviruses currently offer an alternative to avoid falling into phishing through malicious URLs, creating policies where said addresses are detected and access is blocked, before suffering information theft.

3. Damage review: This method works when you fall for a phishing type of attack and serves more to report and prevent further spread of the infection in question. It begins by reviewing the logs of the operating system, the browser or the antivirus, which could gather information from IP addresses to new URLs to add to the Blacklist, focusing on isolating said elements from the network.

4. Establishment of rules in Firewall: In the case of a network in attractive shape and properly structured, it is possible to add information filtering rules through the Firewall, in which the URLs detected in the Blacklist can be added to deny access/ output to the network to them.

Once the functions described above were developed, the blacklist method was tested for blocking malicious QRs (successful blocking in less than 0.5 seconds), for a local query. In the case of analysis and blocking APIs from the virustotal.com and filescan.io sites, a detection response speed was obtained as shown in Table 1, these times are since the query was made in real time using Web services.

CONCLUSIONS

Cybercriminal attacks have diversified from simple viruses and spyware to complex ransomware schemes and QRishing and Quishing attacks. This is because the use of QR codes has become popular as an effective application to quickly access information of all kinds. However, this same accessibility and frequent use has attracted cybercriminals, who can change them or install them in usual places, such as restaurants, ATMs, parking meters, department stores, etc., to attract and steal confidential and financial information from victims. It is important to consider the risks of using this technology.

The attack methods described in this work have allowed attackers to access confidential data, hijack information and destabilize online services, generating an urgent need to develop effective countermeasures, as well as raising user awareness so that they do not provide information. confidentiality that is requested of them when reading these codes.

The current work presents a solution for the validation, verification, and detection of malicious software in QR codes. Characterizing some of the most common attacks. In the tests carried out on the links considered malicious, an exact recognition was obtained, as they were registered on the blacklist. That means, just like an antivirus, if you have the pattern or signature, the malware will be detected, but any significant modification might leave it undetected, therefore manual intervention is required to register a variant of malicious sites. This solution works satisfactorily with the most well-known and registered attacks in Mexico and Latin America, which is the goal pursued. An improvement proposal for the interaction and search for malware information from remote sites would be the use of a Web Proxy system with cache and the use of self-developed tools for the detection and prevention of malware in emails and URLs.

Another recommendation is the implementation of malware (malicious software) detection, prevention, and attack containment systems (known as IDS/IPS), which are an alternative solution that have many advantages to guarantee the security of the information on users and companies.

ACKNOWLEDGMENTS

We would like to thank Alexis Cortés, Rubén Gómez, Christian Y. Aguilar, Alexis Trujillo, Leonardo D. León, Kevin Diaz-Barriga, Moises Equihua, Leonardo Olvera, Israel Senen and José M. Tamayo, students of the Instituto Tecnológico de Morelia, from the Engineering careers in the project, for their participation and support in carrying out the project. Computer Systems and Information and Communication Technologies. Likewise, we thank the Academy of Systems and Computing, for their professional support and infrastructure that allowed us to achieve the results shown. To the Tecnológico Nacional de México, for their authorization to carry out the research project "Caracterización de ataques a códigos QR (medusa; qrishing/ quishing) utilizando malware; software para detección y contención en aplicaciones móviles de México" with code: 21304.24-P and finally to the staff of the UNAM, for their technical support in data analysis, to the MGTI. Atzimba G. López Maldonado, and MTI. Alberto Valencia García from IIES-UNAM.

REFERENCES

1. 90 Grados (2024). Redacción, "Amenaza en seguridad con códigos QR genera pérdidas millonarias: PSI-internacional". https://www.noventagrados.com.mx/tecnologia/amenaza-en-seguridad-con-codigos-qr-genera-perdidas-millonarias-psiinternacional.htm, accessed on 11-2024.

2. Bardají, E. (2022). Cuando el malware se encuentra en la carta del restarante. Retrieved from Cyber Security & IT Solutions: https://www.esedsl.com/blog/cuando-el-malware-se-encuentra-en-la-carta-delrestaurante-cartas-por-codigo-qr

3. Cloudflare (2020). ¿Qué es el quishing? Retrieved from https://www.cloudflare.com/eses/learning/security/what-is-quishing/

4. Eduardo Benavides, W. F. (2020). Caracterización de los ataques de phising y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. Ciencias Informáticas, 97-104.

5. Huidobro, J. M. (2009). Código QR. Qué es…, p. 172-174. Retrieved from /https://cursa.ihmc.us/rid=1NS6XZ211-1V8WNZ2-2555/Microcodigos%20qr.pdf

6. ISO/IEC 27001 (2024). Retrieved from 11-2024, de Information security management systems: https://www.iso.org/standard/27001

7. Itdigitalsecurity (2023). itdigitalsecurity.es. Retrieved from Tres amenazas detrás de los QR: QRishing, QR inverso y QRLjacking: https://www.itdigitalsecurity.es/endpoint/2023/09/tres-amenazas-detras-de-los-qrqrishing-qr-inverso-y-qrljacking

8. Kim, D., Kim, S., Ryu, G., Choi, D. (2024). Session Replication Attack Through QR Code Sniffing in Passkey CTAP Registration. ICT Systems Security and Privacy Protection. SEC 2024. IFIP Advances in Information and Communication Technology, vol 710. Springer, Cham. https://doi.org/10.1007/978-3-031-65175-5_21

9. Nathaly Castro Acuña, M. A. (2019). Análisis de métodos y técnicas existentes para minimizar agujeros de seguridad al usar códigos QR. Revista UIS Ingenierías, 157-173.

10. Statista. (2023). Statista. Retrieved from https://es.statista.com/estadisticas/1233236/porcentaje-usuarios-codigo-qr-mexicotipo-uso/.

11. Ortega, R. (2022). En México el mercado para Código de Barras y QR supera los 90 millones de dólares anuales. Esemanal, accessed on 11-2024

12. Vall, V. (2023). Seguridad de los códigos QR: ¿Es seguro utilizar los códigos QR? Accessed 10-2024 https://www.qrcode-tiger.com/es/qr-code-security

13. Xing Han, Y. Z. (2023). Medusa Attack: Exploring Security Hazards of in-app QR Code Scanning. Proceedings on the 32nd USENIX Security Symposium, (págs. 4607-4626). Anaheim.