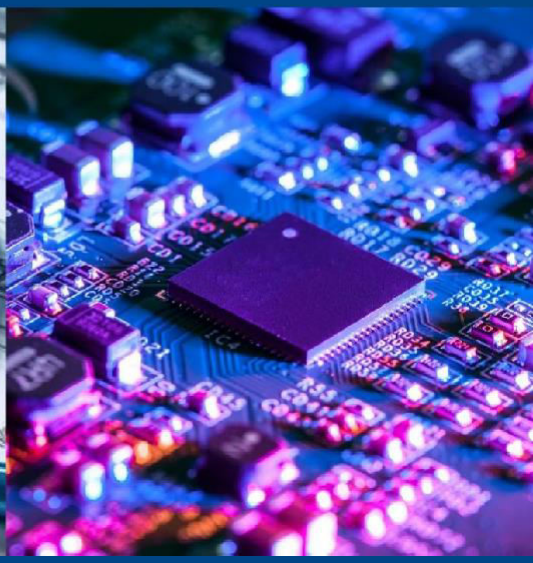
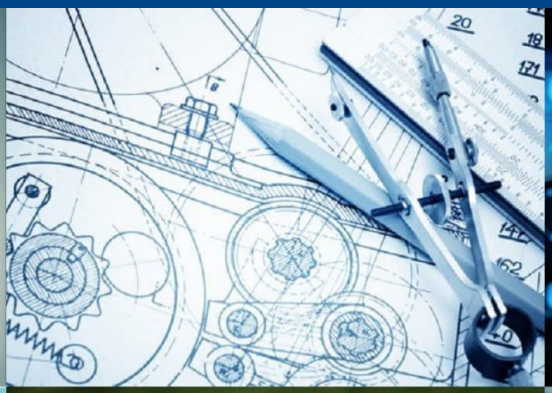
ISSN: 2582-7219

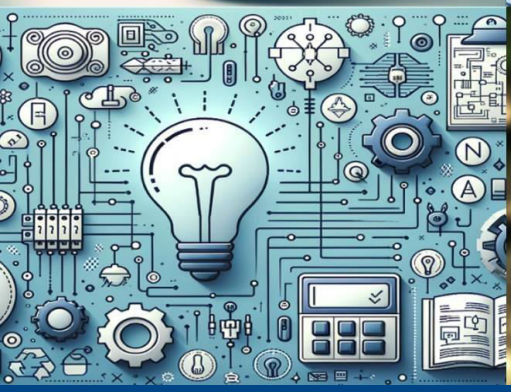




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 7, July 2025**

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807078

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

QR Code Jacking: A Threat to Digital Trust in a Connected World

Anjum Afsana T.A, Dr.Charan K V

M.Tech (CSE) Student, Shreedevi Institute of Engineering and Technology, Tumkur, Karnataka, India

Associate Professor, Dept. of CSE, Shreedevi Institute of Engineering and Technology, Tumkur, Karnataka, India

ABSTRACT: Over the years, QR codes have become a staple in digital engagement acting as direct access points for contextual information and applications. But this broad acceptance has also opened new doors for attackers that farm the trust users place in QR codes. In this paper we investigate QR Code Jacking (QCJacking) which is a kind of cyber-attack that dupes users by changing QR codes and directing them to malevolent websites or phishing pages. In this paper, we simulate how an attacker can exploit QR codes to weave together arbitrary content within them (usually a malicious URL), then automatically force unsuspecting users into accessing dangerous URLs using our Python scripts. Our work unveiled the insecurities directly exposed in using QR codes, and demonstrates how to actually carry these attacks out. Mitigation strategy includes user awareness, secure QR code generation practice and real-time validation for a scanned QR-code. In this paper, we seek to increase the security posture of QR code-based environments by raising awareness about possible attacks that can be used on a manipulated QR code and implementing defensive measures.

KEYWORDS: QR Code Jacking (QCJacking), QR Code Security, Cyber security, URL Masking, Phishing Attacks

I. INTRODUCTION

As the world goes more and more digital, Quick Response (or QR) codes serve as a regular means of generating a quick and easy access to Website addresses, online payment portals, limited time offers, and other forms of internet content. They are user friendly and can be adopted in industries hence making them an efficient means of engaging users. However, as with every advance in technology, a new concern in the usage of QR code has emerged because of the rapid growth in its application. These are the weaknesses whereby the attackers have been able to launch phishing scams that are a type of social engineering where the attacker tries to lure a user into providing him or her sensitive information such as passwords and account numbers by creating fake websites and or sending the user an infected link. The new form of attack has been dubbed as QR code phishing or QC Jacking and it has gradually featured among the most dangerous cyber threats.

QC-Jacking is a form of attack that invents QR codes that seem genuine but when a user scans with his/her smart phone is redirected to fake website or execute unwanted application download. These attacks exploit the trust the users have in the QR codes as they are scanned without much ado. This is because cyber attackers can physically stick the QR codes on a variety of objects like posters or on advertisements or make them available online through social media platforms and emails and trick a number of victims into scanning the codes. Once a user has been infected by the code which has been scanned into a computer, it will take the user to look-alike websites with the intention of making the user provide his or her login details, credit card information or any other information deemed important by the hackers.

This work is inspired mainly by the current surging trends in QR code phishing attacks and the general ignorance of the dangers involved in scanning unfamiliar QR codes. On this score, it is imperative to recognize, QR codes, while relatively expedient are, regularly, an oversight in security for most people and companies. Current safeguards do not sufficiently protect the new threats introduced by QR code management; thereby putting people at risk of identity theft, loss of data, and fraud. Since QR codes are being implemented in important segments like banking, retail, and healthcare, protecting such systems is now an issue.

This research intends to fill this gap by examining the weaknesses that current QR code systems have that enable QR phishing attacks. In particular, the research addresses the QC-Jacking tool which is basically an automated phishing

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

system that takes advantage of the above mentioned weaknesses in order to extract sensitive user information. It describes how exactly, QC-Jacking happens, the tools and techniques, that are deployed in pulling off a phishing assault, and appraises the vulnerability that is inherent in the processes of generating QR code, scanning processes and usage that hackers can capitalize on.

The objectives of this research are:

- Identifying vulnerabilities: In order to explain the shortcomings of the QR code generation and scanning phase which leads to the reality of phishing attacks.
- Demonstrating how vulnerabilities are exploited: In order to explain how these weaknesses can be exploited by the attackers by using tools such as QC-Jacking for the purpose of phishing.
- Evaluating existing security measures: Security experts use research methods to analyze the possibility of new threats regarding existing security measures and how current security measures comprehend new threats such as QR phishing

Thus, this research neither offers solutions for the problem at hand nor detracts from the existing strength of current QR code systems but only elaborates on the existing QR phishing threats and the security flaws transcending current QR code systems. Therefore, the conclusions of this study will form the basis for subsequent investigations as well as subsequent enhancements to security, while putting pressure on industries to become much more active in responding to these emerging risks.

II. sYSTEM OVERVIEW

The block diagram illustrating QC-Jacking is shown in below figure.

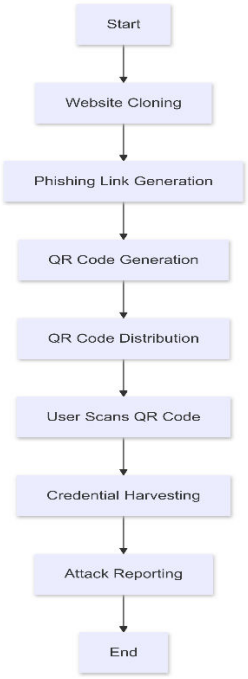


Fig.1. Block Diagram of QC-Jacking

The QC-Jacking tool which is an advanced form of an automated phishing tool threatens the safety of the QR code technology and can facilitate the process of carrying out a massive phishing act. The process starts with cybercriminals capturing replicas of actual sites with the help of certain applications such as Httrack to create mirror copies of reputable sites such as social media, web services, and banking sites. These cloned sites are intended for giving the attackers the opportunity to capture user's sensitive data that they input in those sites. This is followed by creating phishing links to

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

these fake sites and making them popular with help of services such as Cloudflare. These links are then translated into what is known as QR codes and are usually printed, on posters, flyers, through emails and other social media platforms. When the users are scanning these Reliable QR code they are lead to the fake websites where they are being asked to input their credentials. That data is then stored and kept for future use by the attackers of the entered information. The system also has options for assessing the impact of the phishing campaign in which attackers can observe which of the QR codes is being scanned, the number of individuals visiting the fake site, and other attendant credentials. This data is beneficial to the attackers because it assists in making modifications to the attack strategy and increase the effectiveness of the phishing attacks.

III. METHODOLOGY

QR code phishing is a relatively new type of cyber threat, used by attackers to create fake QR codes that can be used to direct users to assorted inherently malicious websites. The common strategy that these attackers' usually employ in order to achieve such attacks usually follow the following process. First, they create phishing websites by copying actual ones with website download tools including Httrack; this makes fake websites to resemble actual ones like social media sites or online banking. The subsequent step after that is to generate a phishing link, once the phishing website is set. This is achieved by services like Cloudflare, it provides services such as port forwarding and public URL generation. This is because the attackers make sure that the phishing website created is well linked to the general public by the use of these public links.

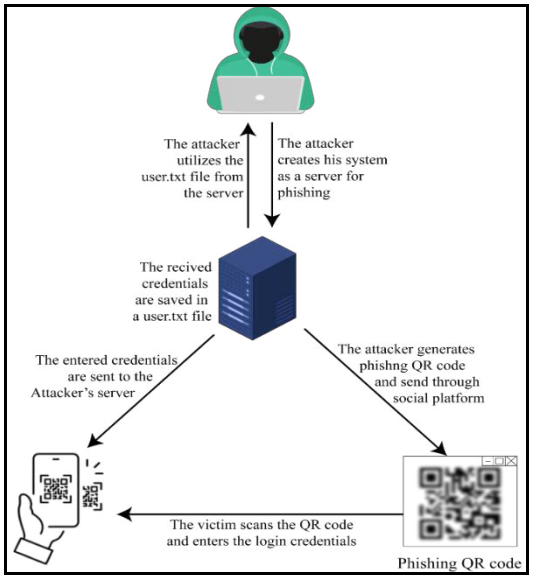


Fig.2. Methodology for QCJacking

After this, attackers translate the phishing link into QR code. This is normally done by means of basic Python scripts that help in converting the perceived phishing URL to a QR code format that can be scanned. These fake QR codes are then placed on different surfaces which include tangible, printed materials such as posters/ brochures and through electronic media including emails and social media platforms, in a way that makes it very easy for users to scan the QR and access the malicious website. A user blindly scans QR codes, sometimes they don't check the URL where the QR code leads them, this makes them penetrate phishing attacks. Some of the underlying techniques that QR code phishing attacks leverage include URL spoofing, in which the actual destination of the QR code is hidden from users, and malware injection where attackers are able to install malware to user's device without their knowledge.

IV. SYSTEM DESIGN AND ARCHITECTURE

The QC-Jacking tool is intended to perform embedded phishing with QR codes; the architecture of the tool is organized in a way that represents an effective five-step system. Details of the attack start with the attacker creating phishing QR

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

codes and delivering them to the targeted users. A user scans these QR codes which leads him to the actual cloned phishing website where his/her login credentials are captured. The attacker compromises the victim's information that could include login details or financial details, and this detail can be used for fraudulent activities including identity theft, unauthorized transactions amongst others. The system makes it possible for all the stages of the attack to be accomplished through automation, and this makes it very easy for the attackers to target as many users as possible at a given interval of time.

Fig. 3. Flowchart of QCJacking

The tools employed in QC – Jacking cuts across a nexus of technologies that enhance phish-assist, and flexibility. PHP is used in the backend to deal with the specific and general credential harvesting as well as the organization of collected data. Python scripts are applied when it comes to automating tasks like creation of QR codes from the phishing links. Cloudflare is also an important ingredient that supports services such as port forwarding to make the phantom sites visible to anyone surfing the web with changed IP address. These technologies collectively co-ordinate the phishing process, starting with the website cloning phase to the attack management phase making the QC-Jacking dangerous efficient phishing tool. Thus, the automated approach in conjunction with using QR codes is a very effective phishing tool, which affects users on various sites and equipment.

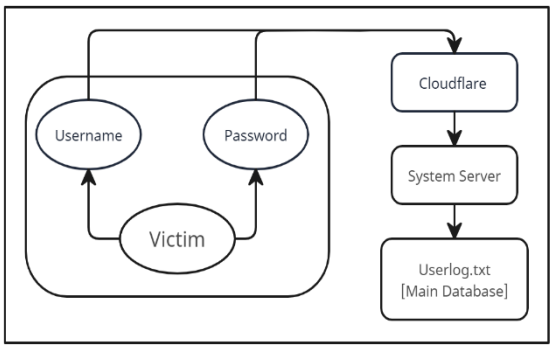


Fig. 4. Backend working of QCJacking

V. RESULTS

The results of the "QC-Jacking: The data of the "An Automated Phishing Tool" project were collected in a formal manner and based on tests and implementations of the use of QR codes in phishing attacks. The results are presented below in the following key areas:

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

1. **System Implementation and Phishing Link Generation:**

- It was also apparent that the tool was capable of creating phishing links through mimicking sites including Instagram and Facebook. As employed by Cloudflare for handling redirection of ports, the phishing links were open and camouflaged to ensure that they would be hard to identify.
- The tool was able to convert these phishing links into **QR codes**, which were stored in PNG format

Fig. 5.1 Generation of Phishing Link

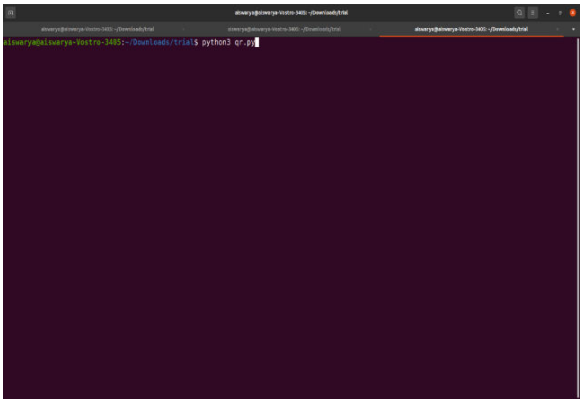


Fig 5.2 The public link will be converted to QR code in png format

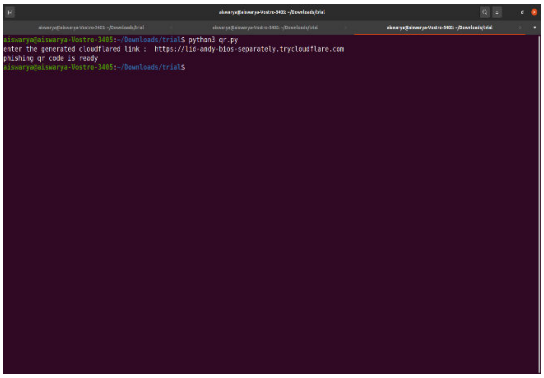


Fig5.3 The generated QR Code will be stored in the current directory.

1. User Interface:

The tool provides a command-line interface that is simple and easy to use. Users can choose from 19 predefined websites to clone, and the process of creating phishing links and QR codes is streamlined

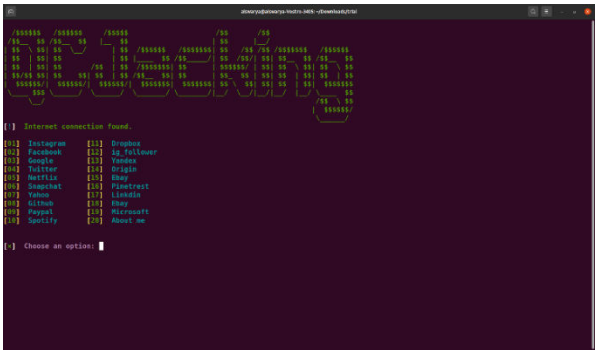


Fig. 5.4 Choose any one of the 19 cloned websites.

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807078

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

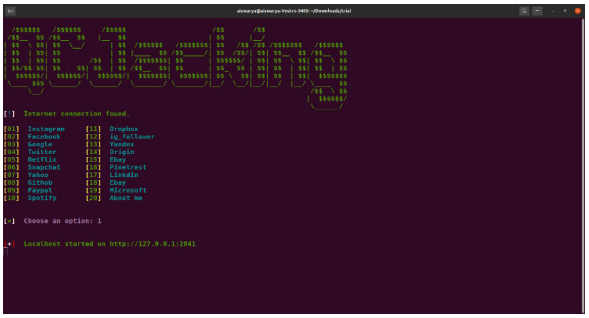


Fig 5.5 Instagram [01] option has been selected to generate the phishing link.

2. Back-End Representation:
Credentials entered by victims were stored on the local server (localhost), and login details were saved securely in the userlog.txt file. This indicates that the tool successfully captured sensitive user data during the phishing attempt

```php
<?php

file_put_contents("userlog.txt",
                  "Instagram Username: " . $_POST['username'] . " Pass: " . $_POST['password'] . "\n",
                   FILE_APPEND);
header('Location: https://instagram.com');
exit();
```

Fig 5.6 Back End Representation for QC-Jacking

3. Attack Execution:
The system demonstrated successful phishing attacks by redirecting victims to cloned websites and collecting their login information once they interacted with the QR codes generated by the tool.

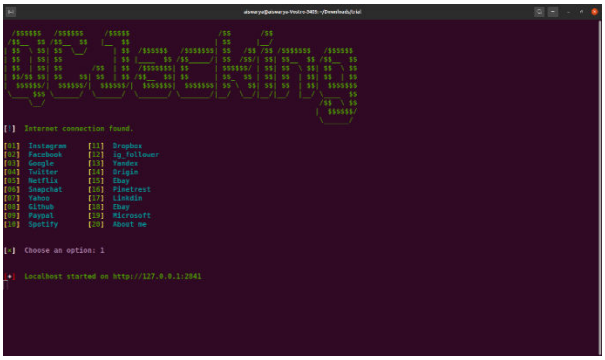


Fig 5.7 Attack of phishing and generation of Phishing QR Code

Attackers were able to gain unauthorized access to victims' accounts, confirming the effectiveness of QC-Jacking in real-world phishing scenarios.

© 2025 IJMRSET | Volume 8, Issue 7, July 2025| DOI:10.15680/IJMRSET.2025.0807078

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

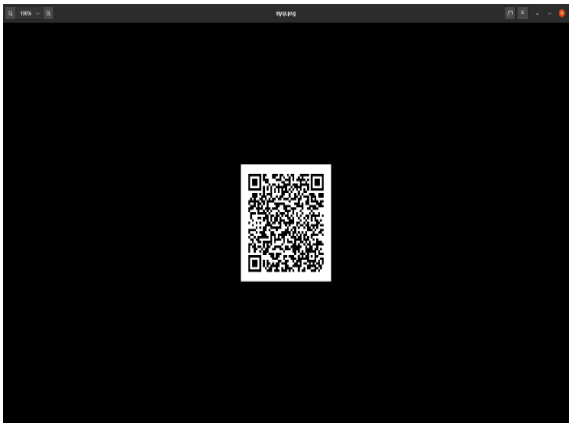


Fig 5.8 This shows the generated QR Code.

VI. CONCLUSION

The target of the QC-Jacking project was achieved as the effectiveness of the QR code phishing, which is a new and growing threat, was shown to be possible and could be done with help of a developed tool. The tool effectively mimicked real websites, created links to the fake sites from which it collected victims' data, and translated the links into QR codes to make the process even sneakier. That phishing attacks can be carried out readily with the help of this tool brings to spotlight the necessity of the use of enhanced security measures and public awareness about QR code based phishing threats. The implications of these findings are clear: they have to put more measures into practice in order to reduce the risks of unauthorized access to such important data – QR code verification systems being the example. Education and employing of anti-phishing tools are also other factors that can help avoid dangers linked with QR code phishing.

VII. FUTURE SCOPE

Mainly considering the factors of technology advancement, it is expected that QR code phishing methods will become more complicated in the future. Future work in this area could explore:

- The features provided by more developed applications and detectors that enable the QR codes to be scanned automatically to check on its link and allow access only if the link is safe.
- AI-based solution for predicting and avoiding phishing attacks while taking into consideration users' habits and common phishing activities.
- Testing different platforms where users interact to check the protection level from the QR code phishing threats for all devices equally.
- Enhancements in the masking identification methods as an approach in an attempt to help security solutions to distinguish the phishing links from realistic ones even if the latter is embedded within the QR codes.

Therefore, through the example of QC-Jacking, the severity of the threats
associated with QR code phishing attacks has demonstrated the imperativeness of the constant developments in cybersecurity measures and awareness. However, it is evident that if due attention is paid followed by an implementation of adequate technology, one can reduce the impact of such phishing attacks to the bare minimum.

REFERENCES

[1] M. Geisler and D. Pöhn, "Hooked: A Real-World Study on QR Code Phishing," *arXiv.org*, vol. abs/2407.16230, Jul. 2024, doi: 10.48550/arxiv.2407.16230.

[2] A. Trivedi, "Phishing Detection in Advanced QR Code Attacks: Challenges and AI-Driven Solutions," *International Journal For Science Technology And Engineering*, vol. 13, no. 1, pp. 479–482, Jan. 2025, doi: 10.22214/ijraset.2025.66306.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[3] K. S. C. Yong, K. L. Chiew, and C. L. Tan, "A survey of the QR code phishing: the current attacks and countermeasures," pp. 1–5, Jun. 2019, doi: 10.1109/ICSCC.2019.8843688.
[4] F. Sharevski, A. Devine, E. Pieroni, and P. Jachim, "Gone Quishing: A Field Study of Phishing with Malicious QR Codes," *arXiv.org*, vol. abs/2204.04086, Apr. 2022, doi: 10.48550/arXiv.2204.04086.
[5] "Gone Quishing: A Field Study of Phishing with Malicious QR Codes," Apr. 2022, doi: 10.48550/arxiv.2204.04086.
[6] G. Raj Charan and D. D. Thilak, "Detection of Phishing Link and QR Code of UPI Transaction using Machine Learning," pp. 658–663, Dec. 2023, doi: 10.1109/icimia60377.2023.10426613.
[7] S. Ismail, M. H. Alkawaz, and A. E. Kumar, "Quick Response Code Validation and Phishing Detection Tool," pp. 261–266, Apr. 2021, doi: 10.1109/ISCAIE51753.2021.9431807.
[8] S. Slamet, "Desain arsitektur aplikasi qr code sebagai anti phishing serangan qr code," *Spirit*, vol. 15, no. 1, May 2023, doi: 10.53567/spirit.v15i1.280.
[9] T. Vidas, E. Owusu, S. Wang, C. Zeng, L. F. Cranor, and N. Christin, "QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks," Springer, Berlin, Heidelberg, 2013, pp. 52–69. doi: 10.1007/978-3-642-41320-9_4.
[10] A. Kasaiani, N. Kushnirenko, O. Troyanskiy, and V. Podufalov, "Method for detecting phishing qr codes using machine learning," *Ìnformatika ta matematičnì metodi v modelûvannì*, Dec. 2023, doi: 10.15276/imms.v13.no3-4.266.
[11] T. Vidas, E. Owusu, S. Wang, C. Zen, and L. F. Cranor, "QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks (CMU-CyLab-12-022)," Nov. 2012, doi: 10.1184/R1/6468011.V1.
[12] H. Huang and S. Pang, "QR code phishing recognition method and system based on URL feature," May 31, 2017

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com