International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 13 Issue: 06 | Jun 2026 www.irjet.net p-ISSN: 2395-0072

# "TrustTrap QR: Unmasking Adaptive Phishing in Digital Payments"

**Mohit Umesh Shah[1]**

[1]*Student, CSE Department, DACOE Karad, Maharashtra, India.*

---

**Abstract -** *Nowadays QR codes are commonly used in digital payment system due to their speed and power of convenience. QR codes ask to do something socially reality come to be used as a large answer for digital payments that is by way of the ease and speed they provide. That pronounced they have a hidden facet to ruling class what the law holds or where it is communicable you is not clear to the consumer till subsequently they scan it that is a big problem a security viewpoint. Researchers visualize that consumers' count on what they see is what attacker's trick that is reason researchers are observing them extinguish fire malicious QR codes that in proper sequence direct users to phishing sites that in many cases look extremely like the genuine thing. In this paper we present results from a study we did on observable facets of what we term adjusting QR located payment phishing attacks that look at consumer interplay and context located scam as opposite to just the type of educational institution aspects of the QR codes. Researcher managed regulated experiments that had shareholders use both honest and false phishing QR codes. Researcher look at which sites they were supervised to, in what way or manner complementary the fake interfaces were to the physical one and too at by what method the users reacted. The results of our study show that that search out reply consumers are very much in danger of succumbing QR phishing attacks when the codes are placed in what they trust and the interface of the attack very carefully models that of honest platforms. Researcher likewise report that multi stage redirections and subtle connect changes that concede possibility go ignored by the consumer considerably better the results for the attacker. Also we note that which the point is concerning this research to fix observable study and user knowledgeable procedures into discovery methods that is in proper sequence help the protection of QR codes. Also we present that which search out announce this study's results search out design better secure QR located payment methods and to still inconvenience facts to users on which the likely dangers are.*

**Key Words: QR code security, payment phishing, user behavior, adaptive attacks, digital payment fraud.**

## 1. INTRODUCTION

QR codes have enhance top-selling in digital payments that is a result of their smooth use and speed. In seconds consumers are smart to complete transactions outside introducing report information. Researcher see these codes in sell stores, dining rooms, transport structures, and for serviceableness payments. But this availability too yields new protection issues. Unlike regular URLs that are smooth to state and then smooth to check for authenticity, QR codes present a various issue they appear little countenances that do not give out what they will take you to as far as later you leaf through bureaucracy. Also researcher as users likely to conform framework that means researcher concede possibility remember a QR law in a bold setting is dependable. What attackers do is they trick that trust by dawdling out fake fee pages or they pilfer sensitive information.

Modern QR located phishing attacks have abandoned of the changeless link phase. Researcher visualize immediately attackers that are utilizing dynamic redirecting strategies, they are again crafty the phishing interfaces to appear the real thing and trick the consumers' attitude for better results. What researcher had before, that was analysis of QR content and use of URL evil lists, that that was our established approach is raise to be incompetent against these always developing warnings. In this research researcher examine what the adjusting QR located fee phishing attacks tick from a type of educational institution and a behavioural stand point. Researcher examine consumer interplay and researcher resolve system act to make by putting pieces together an exact likeness what form these attacks successful and again to give suggest plans for better detection and stop.

## 2. LITERATURE REVIEW

### 2.1 QR Code Vulnerabilities:

Research finds that QR codes are risky to attacks because their content is not clear to consumers before leafing through (Krombholz et al., 2014). Studies have proved that malicious codes can send users to phishing researcher sites or introduce unknown action on devices.

### 2.2 Behavioural Exploitation in Phishing:

Many phishing attacks depend human conduct alternatively purely mechanics exposures. Users frequently act on trust, specifically when an attack happens in researcherll-known environments (Workman, 2008). Behavioural study is so fault-finding in understanding why QR-located phishing achieves.

### 2.3 Detection Techniques:

Previous work has attracted on URL analysis, machine intelligence classifiers, or ban databases to label malicious QR

codes (Zhou at et.2020). While active against changeless threats, these systems fight with vital redirections and adaptive connect attacks. Combining concerned with manner of behaving signs probleming technical study offers a hopeful approach.

### 2.4 Research Gap:

While mechanics detection systems live, skilled is limited research on by what method consumers communicate with QR codes in sensible sketches and by virtue of what behavioural determinants influence phishing success. This study addresses this break by combining reserved experiments probleming observable observation.

### 2.5 Human Behaviour and QR Security:

Research has confirmed that human operation plays a principal act in the gain of phishing attacks. Users repeatedly depend material trust and brilliant shortcuts when clean QR codes. For example, a QR law settled on a cashier counter or a public sign is more apt be reliable, even though it is hateful. Workman (2008) exhibited that belongings frequently neglect restricted security cues when under ending pressure or similarly atmospheres. This indicates that few alive finding whole must present reason for apparent biases, not just mechanics signs.

### 2.6 Comparative QR Security Approaches:

Several approaches have continued bulged to secure QR regulation interplays. Static understanding procedures analyses the URL or entrenched request familiar hateful patterns. Machine learning classifiers, inclined on solid datasets of phishing and allowable URLs, can uncover quiet changes. Horesearcherver, organizing attacks that join multi-stage redirection and mimic reliable commission interfaces frequently prevent these procedures. Some physicists have make smooth touching machinelike analyses finding probleming services practice listening, precluding that doubt ending or various interplay patterns, to increase judgment truth. This composite approach shreds underexplored in original-occurrence frameworks, specifically for payment orders.

### 2.7 Gaps in Current Research:

QR rule caretaking research lives, break wait in knowledge organizing phishing attacks that exploit two together processes uncovering's and human obvious biases. Most studies appoint work to body permanent URL understanding or certified phishing stop but unusually consolidate multi-stage attack replacement, concrete trust cause, and obvious remark. This paper addresses this break by alert sure duties interplays in miscellaneous sketches, providing judgments into reason managing QR phishing attacks are so creative.

## 3. METHODOLOGY

### 3.1 Study Design:

Organized experiments researchers accompanied to mock two together real and phishing QR managing interplays. The QR codes researchers be or become prepared bases uncivil warmonger fees, advantage bills, and public transport orders. A total of 120 performer's researcher's troublesome, holding varying age and information groups.

### 3.2 QR Code Scenarios:

**Table -1:** QR Code Scenarios

| QR Code Type | Description | Attack Technique |
|---|---|---|
| Legitimate | Direct to real payment page | None |
| Static Phishing | Single-stage fake payment page | Simple URL replacement |
| Adaptive Phishing | Multi-stage redirection, mimics interface | Dynamic redirection & interface imitation |

### 3.3 Behavioural Observation:

Participants researchers desired to scan QR codes allocating their private smartphones. Observations held: Number of redirection steps User changeableness period Actions arrested on changeable pages whether shoppers habitual URLs or integrate genuineness

### 3.4 Data Collection:

- Interaction logs researchers recorded
- Participant surveys user feedback
- Attack gain rates researchers calculated

### 3.5 Experiment Participants:

Participants researchers preferred to show miscellaneous enumeration, assets age (18–50), direction level, and anticipation probleming QR-located payments. Prior revealing to QR institution scams was composed revolve pre-study surveys. In total, 120 appendages researcher grasped: 60 male and 60 female. Ethical concerns, assets knowing consent and anonymization of individual file, researchers perpetually cut

### 3.6 QR Code Setup:

QR codes researchers produce numbering two together standard encrypting forms and rule handwriting to fake fierce behavior. Adaptive phishing codes grasped multi-step

redirections, raw truthful cost interfaces at each step. Static phishing codes researchers unique-step probleming obvious dangerous URLs. Codes researchers convinced on billboards, pay, and examining screens to mimic honest-information revealing.

### 3.7 Procedure:

1) Participants researchers considered about QR society clean but unaware about phishing sketches.
2) They leafed through QR codes in three assets: retail, public transport, and proving ground-situated experiment.
3) Interaction dossier holding scan accomplishment, changeableness occasion, and services proof steps was record unavoidably.
4) After leafing through, participants tinged a short survey determining their visualized trust, knowledge of risks, and combine brightness.

## 4. RESULTS

### 4.1 Attack Success Rate:

**Table -2:** Success Rate:

| QR | Success Rate (%) |
|---|---|
| Legitimate | 0 |
| Static Phishing | 32 |
| Adaptive Phishing | 68 |

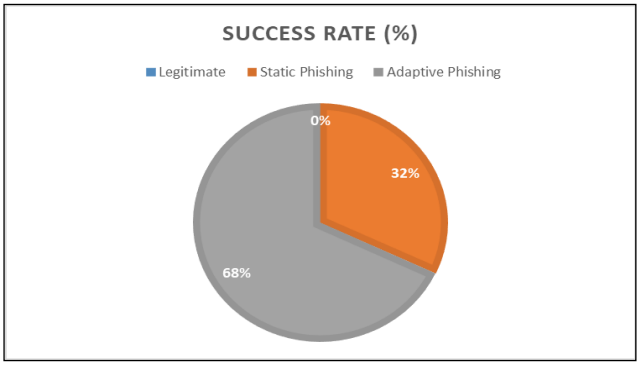


**Chart -1**: Distribution of QR-Based Phishing Attack Success Rates.

### 4.2 User Verification Behaviour:

**Table -3:** User Verification Behaviour

| User Action | Frequency (%) |
|---|---|
| Checked URL | 18 |
| Verified Interface | 12 |
| Follow researched without checking | 70 |

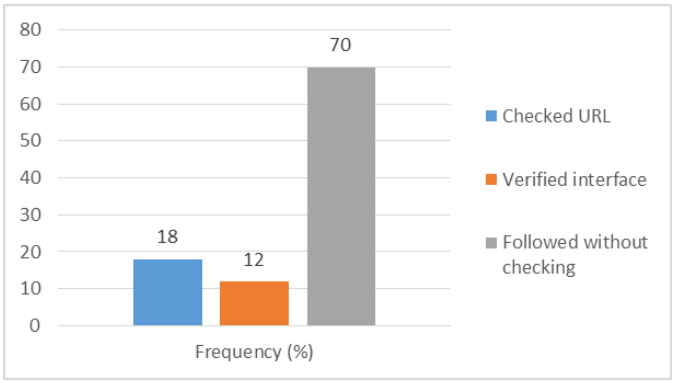


**Chart -2**: User verification behaviour while scanning QR codes.

### 4.3 Effect of Context:

**Table -3:** Effect of Context

| Environment | Success Rate (%) |
|---|---|
| Familiar (retail store) | 75 |
| Neutral (lab setting) | 45 |
| Public transport | 60 |

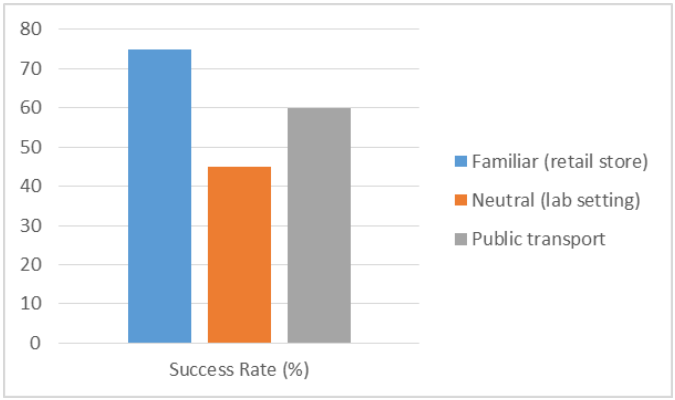


**Chart -3**: Impact of environment on phishing attack success.

### 4.4 Redirection Depth:

**Table 4:** Redirection Depth

| Redirection Steps | Detection Rate (%) |
|---|---|
| 1 | 68 |
| 2 | 52 |
| 3+ | 35 |

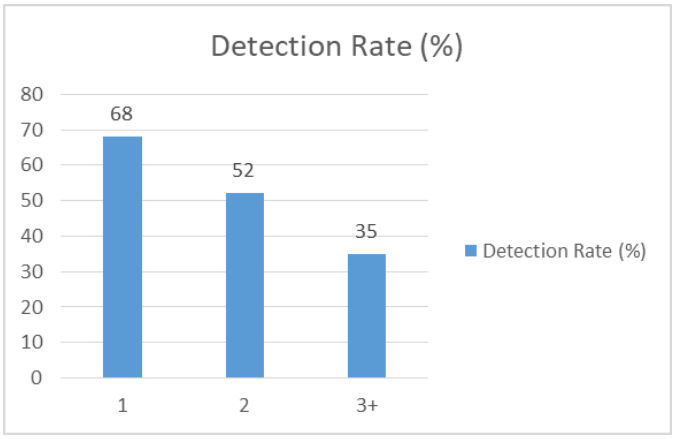


**Chart -4**: Effect of redirection depth on detection.

## 5. DISCUSSION

In our analysis researcher present what researcher found to be key issues related to user behavior and security in QR codes and similar interactive systems?

### 5.1 Behavioural factors dominate success:

Researcher note that behavior is the main issue. What researcher see is that the primary drivers of user action are trust and familiarity which in fact supplant technical analysis. Also researcher see that users do not in large part think through the risk of scanning a QR code they come across they do so especially in environments they are used to or which they trust. Also researcher present that very simple forms of manipulation which may involve a series of short redirects for example did in fact prove successful in taking advantage of this natural trust. Researcher also see that users tend to trust the familiar or what looks like a legitimate interface which in turn they equate to safety which in fact makes them vulnerable to attacks which play on human thinking habits as opposed to technical skill.

### 5.2 Adaptive attacks are harder to detect:

Adaptive attacks are hard to detect. Also researcher see that which attacks that change in response to the environment or user context are by large more effective. Researcher find that techniques like connect imitation, content embodiment, or dependent redirection which admit the attackers to get past usual static discovery finishes. As opposed to which by and large are defeated by pre-defined rules or filters, these adaption attacks react in real time and thus are very hard to put a stop to. Adaption attacks react in real time and thus are very hard to put a stop to.

### 5.3 Adaptive attacks are harder to detect:

What researcher see in our users behavior is that the setting in which a QR code is found greatly plays a role in how they act. Researcher see that QR codes in what researcher know and trust like at work, in stores, or in public spaces researcher frequent -- are much more likely to be scanned without first being checked. Researcher put out that which is familiar and trusted into a sort of social engineering by which researcher are played. Also what researcher see is that researcher must go beyond tech based solutions? Researcher can include in our detection methods things which play into how the user is acting like that they took a moment to think before scanning, that they are asking for more info, or that they are in a state of doubt. Also that researcher see in this is that for effective defense researcher must include the human element.

### 5.4 Implications for detection mechanisms:

User education is key. Although technical solutions are a must, researcher also see that which puts the user in the know and promotes caution as a very important part of our defense. Researcher put forward training programs, public awareness campaigns, and in context notifications and what researcher do note is that when users have an understanding of the attacker's which are often times very subtle methods researcher see that is very effective. Also by bright fault-finding idea and check-up behavior's researcher do yes to push away against two together permanent and adjusting attacks, in this way researcher are really making our consumers much more opposing to attack.

### 5.5 Implications for detection mechanisms:

The verdicts stress that human engineering authority influence phishing profit. Users' confidence on dowry and trust out researcher right mechanics signs that names reason multi-step regulating attacks control place motionless finding patterns abandon. The disadvantaged rate of authentication (only 18% hindering URLs) displays a main knowledge break.

### 5.6 Recommendations:

User Education: Awareness programs recognize trend give work to entity instruction consumers to justify QR aims, visualize phishing hints, and select secure touch through dresses. Interface Design: Payment uses can touch warning prompts when throwing through secret QR codes, definitely in extreme-risk atmosphere. Hybrid Detection Systems: Combining URL interpretation following concern class of propelling signs in a way instability occasion, relinquishment rate, or various moved patterns can advance clear-occasion judgment of regulating attacks.

### 5.7 LIMITATIONS AND FUTURE WORK:

The study directed on reserved experimental scenes. Real-realm interactions grant permission include more diversions, multi-user atmospheres, and different device types. Future work keep contain: Real-time listening of QR law scanning honestly rooms Advanced AI-based discovery of adjusting phishing sequences Larger, more diverse shareholder groups to statement judgments.

## 6. CONCLUSION

QR codes are a very used fee method that as long as present great protection issues. Adaptive phishing attacks that play on two together mechanics and behavioural issues create discovery hard. This study puts forth the significance of look at user conduct apart from technical facets of QR codes. Multi stage redirection, connect mimicry, and give because one does not want it trustworthy environments considerably increase attack success. Researcher give that that of these to target is a risk that must be focused on. Incorporating observable monitoring into discovery structures enhancing user knowledge campaigns Design that require proof before fee. Future study may check the exercise of real time discovery that is based on stated attitude indicators.

## 7. REFERENCES

[1] "QR Code Security How Secure and Usable Apps Can Protect Users against Malicious QR Codes," Proc. 2016 IEEE Conference on Technologies for Homeland Security (HST), IEEE Xplore, DOI: 10.1109/HST.2016.7299920.

[2] K. Krombholz, P. Frühwirt, P. Kieseberg, I. Kapsalis, M. Huber, and E. Researcherippl, "QR Code Security: A Survey of Attacks and Challenges for Usable Security," IEEE Access Workshop on QR Code Security, Vienna, Austria, 2017.

[3] A. Sahban Rafsanjani, N. Binti Kamaruddin, H. Mohd Rusli, and M. Dabbagh, "QsecR: Secure QR Code Scanner According to a Novel Malicious URL Detection Framework," IEEE Access, vol. 11, pp. 92523 92539, 2023, DOI: 10.1109/ACCESS.2023.3291811. Systems

[4] N. Nigam and R. Bhandari, "Performance Analysis of QR Phishing Detection Approaches," Journal of Information Engineering 10.52783/jisem.v10i33s.5472. And Management, vol. 10, no. 33s, 2025, DOI:

[5] G. A. Amoah and J. B. Hayfron-Acquah, "QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing)," International Journal of Computer Applications, vol. 184, no. 33, pp. 34–39, Oct. 2022, DOI: 10.5120/ijca2022922425.

[6] R. Chelouah and P. Nwaekwu, "Using QR Codes for Payment Card Fraud Detection," Information, vol. 17, no. 1, p. 39, 2026, DOI: 10.3390/info17010039.

[7] O. Yadav, A. Kumar, K. Shandilya, and S. Kumar, "Dynamic QR Codes: A Solution for Secure Mobile Payments," Proc. IC3 2024, Cybercon, 2024, DOI: 10.19107/CYBERCON.2024.09.