QR Code Integrity by Design

Luka Bekavac
luka.bekavac@student.unisg.ch
University of St.Gallen
St. Gallen, Switzerland

Simon Mayer
simon.mayer@unisg.ch
University of St.Gallen
St. Gallen, Switzerland

Jannis Strecker
jannisrene.strecker@unisg.ch
University of St.Gallen
St. Gallen, Switzerland

Figure 1: All posters used in the first user study at the Christmas market. From left to right (a) StandardQR tampered (b) StandardQR (c) SafeQR (d) SafeQR tampered.

ABSTRACT

As QR codes become ubiquitous in various applications and places, their susceptibility to tampering, known as quishing, poses a significant threat to user security. In this paper we introduce SafeQR codes that address this challenge by introducing innovative design strategies to enhance QR code security. Leveraging visual elements and secure design principles, the project aims to make tampering more noticeable, thereby empowering users to recognize and avoid potential phishing threats. Further, we highlight the limitations of current user-education methods in combating quishing and propose different attacker models tailored to address quishing attacks. In addition, we introduce a multi-faceted defense strategy that merges design innovation with user vigilance. Through a user study, we demonstrate the efficacy of 'Integrity by Design' QR codes. These innovatively designed QR codes significantly raise user suspicion in case of tampering and effectively reduce the likelihood of successful quishing attacks.

CCS CONCEPTS

• **Security and privacy → phishing**; **Usability in security and privacy**.

CHI EA '24, May 11–16, 2024, Honolulu, HI, USA

ACM ISBN 979-8-4007-0331-7/24/05
https://doi.org/10.1145/3613905.3651006

KEYWORDS

quishing, QR codes, QR code based phishing, phishing susceptibility, privacy

ACM Reference Format:
Luka Bekavac, Simon Mayer, and Jannis Strecker. 2024. QR Code Integrity by Design. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA '24), May 11–16, 2024, Honolulu, HI, USA.* ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3613905.3651006

1 INTRODUCTION

In the current digital landscape, QR codes have become an integral tool, transforming how we engage with objects, businesses and services. Their convenience has led to widespread use, from viewing restaurant menus and buying concert tickets to managing parking payments.[4] However, this ubiquity has also attracted malicious exploitation, leading to the emergence of a phenomenon that is commonly referred to as *quishing*: QR code-based phishing. quishing involves the fraudulent manipulation of QR codes to mislead users into engaging in harmful activities, potentially leading to theft of personal data and even financial loss. The European Union Agency for Cybersecurity (ENISA) Threat Landscape report acknowledges the increasing problematic issue of quishing, highlighting its prevalence and the sophisticated tactics employed by attackers [3, p. 76-77]. The report mentions different cases where QR codes are used as a vector for attacks. These include distributing fake delivery notice slips purportedly from the French postal service, targeting individuals in San Francisco with counterfeit parking tickets, and a case in Northern California where a young individual was arrested for placing fake parking tickets on cars near a beach. Additionally, a significant incident in Singapore involved a victim

losing $20,000 after scanning a malicious QR code in a bubble tea shop.

Current solutions to combat malicious QR code threats have largely focused on raising user awareness. While educating users on the risks is undeniably valuable, this approach often disproportionately impacts those who are already disadvantaged, deepening the digital divide. Those without access to educational resources or technological literacy are left more vulnerable. In contrast, a more direct and instinctive approach lies in the innovation of QR code design itself. By proposing visual design patterns that lead to the creation of QR codes where tampering can be detected more easily, we can facilitate the immediate recognition of potential threats. This method does not rely on specialized knowledge or technological tools, thus not disadvantaging individuals based on their socio-economic status. Implementing such design innovations can create a safer digital environment for all users, regardless of their educational background or financial capabilities, ensuring equitable access to digital safety measures.

We propose that the incorporation of easily recognizable designs, symbols, or patterns into QR codes can make tampering or alterations recognizable. For example, a brand embedding its distinctive logo within the QR pattern means any disturbance or alteration in this logo would be a clear sign of tampering. Such visual cues incorporated into the QR code design would act as a first line of defense. This is not just about aesthetics but about harnessing design for security. It allows non-tech-savvy users to spot discrepancies, making the act of scanning QR codes a safer and more reliable interaction. This approach ensures that the security of QR codes isn't solely a behind-the-scenes technical effort but is also visually evident, empowering users in the scanning process.

Our work makes contributions by:

- **Proposing various attacker models:** We have identified and categorized potential threat actors, providing an overview that enhances the understanding of security threats specific to QR codes.
- **Developing defense strategies:** We have crafted a range of targeted defense strategies in response to the attacker models we have identified, reinforcing QR code security against various vulnerabilities.
- **Conducting a user study for validation:** To substantiate our proposals, we have accompanied our strategies with an user study. This study validates the effectiveness of our defense mechanisms, providing empirical evidence of their impact on enhancing QR code security.

2 RELATED WORK

Much research has been done in the field of phishing attacks, while only a few studies have focused on quishing specifically.

Building upon the work of Krombholz et al. [6], who touched on the security vulnerabilities of QR codes in the context of phishing threats, our project has taken these initial insights to a more developed stage. Krombholz et al. put forth the notion that incorporating complex visual elements into QR codes, such as detailed color schemes, might help users detect tampering in urban settings. They speculated that a QR code with a more intricate design would be more difficult for an attacker to modify discreetly and suggested that the integration of these complex visuals into the advertisement's color scheme could be a deterrent. However, they did not delve into specific design strategies or investigate this concept further. Our research takes Krombholz et al.'s preliminary idea as a starting point and extends this concept by specifically targeting the issue of quishing attacks and systematically categorizing attacker models to tailor defense strategies, thus addressing a more nuanced aspect of QR code security and user interaction.

Another contribution to quishing comes from Sharevski et al. [11], who investigated the phenomenon of quishing, or phishing via malicious QR codes, during the COVID-19 pandemic. In their study they explored user behavior and susceptibility to quishing through a study with 173 participants simulating a COVID-19 digital passport sign-up with a malicious QR code. They found a significant tendency among participants to fall for quishing, and developed the quishing Awareness Scale (QAS) to assess participants' awareness of quishing threats. The study's results helped in proposing quishing awareness training guidelines and developing usable security indicators to warn users about quishing threats, providing valuable insights into user behavior and education strategies to combat attacks.

Recognizing the need for a more robust defense against quishing, the study by Mavroeidis and Nicho [8] shows how quishing attacks are carried out and proposes the QRCS model, a server-client architecture that enhances QR code security through hashing and digital signatures. Their solution, QRCS (Quick Response Code Secure), leverages digital signatures and cryptographically secure hash functions like SHA-2 or SHA-3 to ensure the integrity and authenticity of QR codes. This server-side platform allows entities to generate digitally signed QR codes, while the client-side application is responsible for decoding, decrypting and verifying the signatures, ensuring that users are directed only to intended sites. Mavroeidis and Nicho's approach marks a step towards securing QR codes against phishing attacks, focusing on the cryptographic validation of QR codes' origin and integrity.

It is important to highlight certain limitations in commonly proposed user education methods for combating quishing. Recommendations found in articles [12] or videos [14], such as verifying the URL before accessing a QR code linked website are less effective against tools such as TinyURL [1] and dynamic links, which obscure the destination URL. Proposed tips for self-protection, such as those suggested by the Federal Bureau of Investigation [9], are not necessarily in harmony with industry trends and QR code providers that advocate the use of dynamic URLs, emphasizing their convenience and advantages [2]. Moreover, the QRCS framework suggested by Mavroeidis and Nicho [8] advocates for the establishment of a new standard and application dedicated to verifying the authenticity and integrity of QR codes. The defense strategies presented in our work concentrate solely on securing the existing QR code standard and its implementation.

3 ATTACKER MODELS AND DEFENSE STRATEGIES

In this section, we delve into the categorization of attacker models and the development of design-focused defense strategies, building

[1] https://tinyurl.com/app (accessed March 13, 2024).

upon our foundational understanding of phishing attacks and their key parameters.

3.1 Foundation

As discussed by Abbasi et al. [1], phishing susceptibility can be predicted using a funnel model, akin to models used in marketing and web analytics to represent a series of interrelated decisions. Their proposed phishing Funnel Model (PFM) captures the progressively dangerous decisions a user faces when encountering a phishing attack, whether through email, search engine results, or social media. This model outlines four critical stages:

- **Visit**: The initial decision involves whether the user chooses to click on a phishing link, leading them to the fraudulent website.
- **Browse**: Upon visiting the website, the user must decide whether to engage with the site, which involves browsing behavior like time spent on the page or the number of pages viewed.
- **Consider Legitimate**: Users who browse the site must then determine if they perceive the site as legitimate, a crucial precursor to considering any form of transaction.
- **Intend to Transact**: The final and most hazardous stage involves deciding whether to transact with the website, leading to identity theft or financial loss.

During their study, the authors observed a narrowing of the funnel, indicative of participants' ability to recognize the phishing scam as they progressed through the stages. The observed loss of participants from stage to stage was significant, with the numbers decreasing from 52.2% at the initial stage to 3.8% at the transaction decision stage. This demonstrates a considerable drop-off at each stage, highlighting the users' increasing ability to identify and avoid the scam as they move further down the funnel.

Transitioning from traditional phishing to quishing, we note that while the attack mechanism is similar, the medium of execution differs. Instead of a deceptive link in an email, quishing uses a QR code as the gateway to the phishing scam, representing a unique challenge in the first phase of the attack funnel. In alignment with our research, we aim to leverage the *QR code integrity by design* approach to further constrict the funnel, diminishing the number of individuals susceptible to phishing. Positioned at the very start of the funnel, our enhanced QR codes are designed to be more likely recognized as tampered by users, leading to a reduced number of scans and, consequently, a more constricted visit phase. This effect cascades through the subsequent stages, promising a narrower funnel overall and a significant reduction in successful phishing attacks.

Vishwanath et al. [13] present the Suspicion, Cognition, and Automaticity Model (SCAM) in their study, which aims to understand and predict individual susceptibility to phishing attacks by considering cognitive, preconscious, and automatic processes. The model highlights the role of suspicion, cognition, and automaticity in the context of phishing. Suspicion is pinpointed as a critical factor. Lyons et al. define it as the degree of uncertainty one feels when interacting with a stimulus, like a phishing email [7]. Moderate amounts of suspicion can significantly improve deception-detection accuracy, as it's fundamental to detecting deception and highly sensitive as a measure of deception-detection. Building on the SCAM, the research further validated the model's effectiveness in predicting phishing susceptibility [13]. In the context of the link attack, individuals who exhibited a higher level of suspicion were significantly less likely to be phished compared to their less suspicious counterparts. Similarly, during the attachment attack, suspicious individuals were significantly less likely to be phished than those who were not suspicious. These findings strongly support the hypothesis that suspicion acts as a protective factor against phishing, underscoring the significance of fostering a critical and questioning mindset when interacting with potential phishing content.

Incorporating the concept of suspicion into our research and proposed defense strategies in Sect. 3.3 is critical, as it aligns with the core objective of enhancing QR code security through design. As proposed later on, by embedding distinct design elements into QR codes, we make tampering noticeable, thereby instigating a state of heightened suspicion among users. This induced suspicion acts as a cognitive trigger, encouraging users to engage in systematic processing and critical evaluation, which significantly aids in the early detection and avoidance of phishing attacks in the browse phase. The practical application of raising user suspicion in tampered QR codes which have been bolstered with defense strategies, is examined and validated in our user study detailed in Sect. 4.

3.2 Attacker Models

In this section, we introduce a new categorization for attackers in quishing attacks, dividing them into three distinct categories based on their operational methods and sophistication levels. The existing literature on phishing and quishing often lacks a breakdown of attacker profiles, a gap this categorization aims to fill. Recognizing and understanding these distinct attacker models is essential for the development of robust defense strategies. The importance of this classification lies in its ability to shed light on the varying threats posed by different types of attackers, thereby guiding the creation of tailored countermeasures against each category. For an overview of these proposed attacker models, see Table 1.

With the increase in the strength of the attacker, stronger protection models are needed. However, it is important to acknowledge that beyond a certain point of attacker proficiency, such as a professional attacker who fakes an entire poster and redistributes it, current proposed defense methods fall short. This highlights the continuous arms race between attackers and defenders in the realm of phishing. While a range of attacker types exist, it is often the case that quishing attacks observed in the field may be associated with what we refer to as Basic Attackers. These attackers can tamper with hundreds of posters in a relatively short amount of time, using standard simple black and white QR codes, though comprehensive data on the prevalence of such attacks is still being developed. This underlines the critical need for effective countermeasures even at the most fundamental level of quishing attacks. Further research is needed to substantiate the frequency and impact of these attacks fully.

Table 1: Attacker models for quishing attacks

Attacker Strength	Characteristics	Methods
Basic Attacker (Opportunistic Attacker)	The *Basic Attacker* possesses limited technical knowledge and resources, relying primarily on easily accessible tools and methods.	Their tactics often involve replacing existing QR codes with fake ones, with little effort put into concealment or targeting. This approach is largely opportunistic, aiming for volume over precision, in the hope that some users will fall for the scam.
Advanced Attacker (Targeted Attacker)	Possessing a moderate level of skill, *Advanced Attackers* have access to more sophisticated tools and a basic understanding of phishing, scams and the user psychology behind it.	They create more convincing fake QR codes, sometimes mimicking the design of legitimate codes from reputable entities. These attackers might also employ basic social engineering techniques, strategically placing the QR codes in semi-private areas to lure specific user groups.
Professional Attacker (Strategic Attacker)	Highly skilled and resourceful, *Professional Attackers* use advanced tools and techniques, with a thorough understanding of security systems and user psychology.	Their approach integrates fake QR codes into complex phishing campaigns, utilizing advanced social engineering, context-aware placement, and timing their attacks to align with relevant events. This category represents the highest degree of strategic sophistication in quishing attacks.

3.3 Defense Strategies

In response to the diverse threats posed by the different attacker models described in Sect. 3.2, we recommend a range of distinct defense strategies and secure QR code implementations. These strategies are informed by the foundational insights discussed in Sect. 3.1 and aim to raise user suspicion, ultimately aiding the user to determine a phishing attack in the first to stages visit and browse. These defense strategies primarily focus on the *Integrity by Design* approach to enhancing QR code security, emphasizing preventative measures incorporated into the design of QR codes and their presentation.The following designs are proposed by us to enhance the integrity of the posters and QR codes:

3.3.1 QR-Art Post Stamping. One approach is QR-Art Post Stamping, where QR codes are seamlessly integrated into artwork or promotional designs. Such integration makes it difficult for attackers to tamper with the code without it being noticeable. As illustrated in Fig. 2, the poster features a QR-Art generated design in which the QR code is an integral part of the overall image.

3.3.2 Multi-Layered QR codes. Another strategy involves crafting QR codes with multiple layers, each containing a segment of the complete QR information. This transforms the QR code into a 3D object, making simple 2D tampering ineffective. The production of such QR codes is possible by using a 3D-printer[2] or laser-cutter.[3]

3.3.3 Embedding the QR code with a transparent background. Instead of standard JPEG or PNG file with white background, QR codes should be integrated as SVG or PNG file, which have a transparent background and are thus more challenging to counterfeit. It is important that the background of the poster should depict something which goes over the area of the SVG/PNG QR code so that tampering is noticed. The poster used during the user study in the paper depict this as it can be seen in the Appendix Figure 1

3.3.4 Custom Sizes for QR codes. Using custom sizes for QR codes on posters can also enhance security. Standard QR code sizes (e.g., 2cm, 10cm, 100cm) as proposed by QR code websites[4], make it easy for attackers to replace them. Custom-sized codes reduce the likelihood of successful tampering or make tampering more obvious. If the fake QR code sticker only covers part of the real QR code or areas around the QR code are also covered by the sticker, the design and look of the poster will be affected by it.

3.3.5 Integrating Design Elements. Incorporating design elements that span both the poster and the QR code can make it visually easier to detect changes or tampering. This could involve using icons, objects or text that overlap with the QR code. The conducted user study described in Sect.4 uses this defense technique depicting a Santa Claus hat or graduation hat which sits on the QR code in Fig. 3. The tampered QR code is cutting off the hat, disturbing the look of the poster.

In order to protect poster and QR codes against Basic Attackers defense strategies like proposed in Sect. 3.3.3, Sect. 3.3.4, and Sect. 3.3.5 are recommended because they are feasible to implement without much additional effort during the creation of the QR code poster. For *Advanced* and *Professional Attackers* the proposed defense strategies in Sect. 3.3.1 and Sect. 3.3.2 are recommended. These are more effortful to incorporate, but thus also harder to fake and copy.

3.4 User Categories

Phishing attacks and fraud schemes are influenced by a multitude of factors and parameters that extend beyond just the technological aspects of websites, emails, and other media. These factors also encompass elements directly related to users themselves. Gavett et al. [5] in their study highlighted that various user-centric parameters significantly impact the effectiveness of phishing attacks. These parameters include age group, distinguishing between older and

[2]See, e.g., https://www.printables.com/model/155573-wifi-qr-code-sign (accessed March 13, 2024).
[3]See, e.g., https://www.instructables.com/Laser-Cut-QR-Codes/ (accessed March 13, 2024).
[4]See, e.g., https://qrplanet.com/help/article/what-is-the-minimum-size-of-a-qr-code (accessed March 13, 2024).

Figure 2: A poster created with https://quickqr.art/ showcasing the defense strategy proposed in 3.3.1

Figure 3: A poster used in the study that implements defense strategies of a SafeQR code.

younger individuals; sex; education level; race; ethnicity; as well as the user's prior knowledge of phishing tactics and their previous experiences of being targeted or falling victim to phishing.

Research indicates that user knowledge of computer and Internet security, including their experience and education in these areas, plays a crucial role in reducing their susceptibility to phishing attacks. This is supported by findings suggesting that greater awareness of online threats enhances the ability to detect and avoid phishing schemes [10].

This underlines the complexity of phishing schemes and the necessity of considering a diverse range of user characteristics to understand and mitigate the risks effectively.

The defense strategies proposed in Sect. 3.3 aim to address and protect users across all demographics and Information and communication technology(ICT) proficiency levels. These strategies, particularly the visual safety elements incorporated in QR codes, are designed to be identifiable by a wide range of users. The detection of tampering in QR codes is made possible irrespective of the user's demographic or ICT-related factors as no prior knowledge or training is needed to spot visual inconsistencies in the design of posters. This makes the approach universally applicable and equally effective for all users, ensuring comprehensive protection against phishing attacks and related security threats. However, it is important to note that further evaluation is necessary to confirm the effectiveness of this strategy across different user groups. As it stands, the assumption that this method is universally perceptible and effective has not been empirically verified.

4 EVALUATION

In order to evaluate the approach of securing QR codes by design, we conducted a user study. This user study aimed to address the following research question: "Can 'Integrity by Design' prevent users from falling victim to quishing attacks?". Our hypothesis concerning the research question is: "Users are more likely to build suspicion when interacting with tampered QR codes that are enhanced with advanced security features (referred to as SafeQR), rather than when interacting with tampered standard QR codes".

To test this hypothesis, we designed four distinct types of posters:

(1) The **StandardQR poster** features a typical white QR code.
(2) The **StandardQR tampered poster** mirrors the StandardQR poster but is tampered another overlaid QR code.
(3) The **SafeQR poster** incorporates the defense methods proposed in Sect. 3.3.3 and Sect. 3.3.5 over the QR code.
(4) The **SafeQR tampered poster** mirrors the SafeQR poster but is tampered with another overlaid QR code.

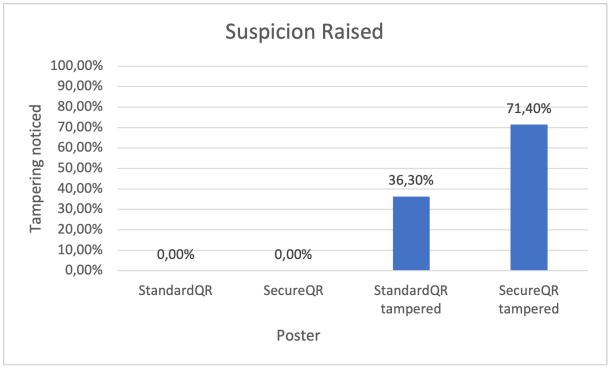
Since the user study was conducted in a German-speaking region, we designed our posters in German to ensure inclusivity and to maximize engagement with a broad range of potential participants. To collect comprehensive and representative data, all posters were prominently displayed at equally accessible and popular locations at both a Christmas market and a university. At the market, we selected a booth set up in a well-trafficked open area, and at the university, we placed the posters on frequently visited poster pinboard walls throughout various buildings.

For the purposes of this paper, all elements of the study, including the questions, have been translated into English. The posters, depicted in Fig. 1 encourage people to scan the QR codes, assessing whether concerns about safety deter them from scanning or raise their suspicion. To motivate scanning, an extrinsic incentive is offered, namely "Scan for a chance to win a voucher for the Christmas market" or "Scan for tips & tricks for the examination phase". The QR code in each poster lead to a user study, and the link is displayed as shortened URL only displaying QRCO.de/id-of-the-code. This choice intentionally strips away checking the URL as a security indicator that participants might use to detect a quishing attack, leading them to rely solely on the poster's design as a cue for security.

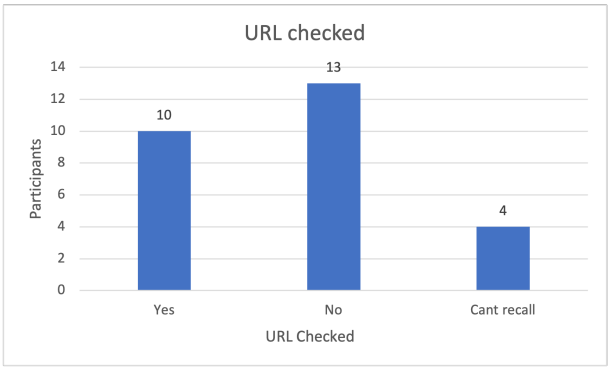
Table 2: The questions from the user study. These are partially derived from the quishing Awareness Scale (QAS) and the Security Behavior Intentions Scale (SeBIS).

No.	question
1	Did you notice anything suspicious about the poster/QR code before scanning it?
2	Did you pay attention to the URL/internet address before scanning?
3	How familiar are you with digital media & devices?
4	How good is your knowledge about phishing attacks?

Upon scanning the QR code, participants are first informed about the study and to keep the nature of the study private to avoid distorting the results. The study is comprised out of four short questions depicted in Table 2. For question 1 and question 2 the Participants could choose between the options 'Yes', 'No', and 'Can't recall'. For question 3 and question 4 Participants could choose on a 5-point Likert scale their familiarity with the topic. The questions are centered around the quishing Awareness Scale (QAS), adapted from the Security Behavior Intentions Scale (SeBIS) by Sharevski et al. [11], to gauge participants' awareness and behavioral responses to potentially malicious QR codes. The QAS, a derivative of the SeBIS's proactive awareness sub-scale, specifically targets behaviors around QR code security.



(a) The results of question 1



(b) The results of question 2

Figure 4: The questionnaire responses on raised user suspicion (a) and URL checking awareness (b).

4.1 Inferred Robustness Against QR code Tampering

Implementing the security measures outlined in Sect. 3.3 intends to enhance the robustness of QR codes against tampering. While time constraints prevented empirical testing, it is reasonable to infer that these strategies would complicate an attacker's ability to subtly alter posters, as they would need to also fake or copy the defense strategies incorporated. This contrasts with the current situation where an attacker can easily generate and print a standard QR code to compromise various posters.

4.2 Quantitative Results

The quantitative analysis from the user study indicates the effectiveness of the security measures incorporated in the SafeQR posters. Throughout the duration of the study a total of 39 scans were recorded across the eight posters deployed. This approach did not involve recruiting a specific number of participants in a controlled setting. Rather, it allowed for spontaneous interaction from market attendees and people walking by, thereby reflecting genuine user responses in a real-world scenario. The data confirmed that no single device scanned a QR code more than once, thus ensuring the reliability of the collected data. Impressively, 69% of the participants

chose to complete the optional survey, reflecting a strong level of engagement with the study.

The results demonstrate that users were more adept at recognizing and reacting to tampering in QR codes that were enhanced with the security measures detailed in Sect. 3.3. This is particularly evident as 71% of the participants identified the tampered SafeQR posters as suspicious, in stark contrast to only 36% for the tampered StandardQR posters, as seen in Fig. 4a.

The study also sheds light on user behavior and their level of awareness concerning digital media and phishing threats. As seen in Fig. 4b, the fact that 37% of the participants actively checked URLs before engaging further implies a degree of vigilance, yet also suggests the need for broader educational measures, as a significant portion did not take this precautionary step. Moreover, over 92% of participants expressed a high degree of familiarity with digital media and devices, but their self-assessed knowledge regarding phishing attacks varied, with 37% rating their understanding as moderate. This points to an opportunity to increase educational outreach and resources to enhance public awareness and understanding of phishing threats.

The quantitative results support the hypothesis that 'Integrity by Design' markedly improves user detection and response to QR code tampering, representing an effective strategy in countering quishing attacks. The insights gained underscore the value of advanced security features in QR codes as a preventive measure against digital security threats and emphasize the ongoing need for comprehensive education and awareness initiatives in the realm of digital security.

It should be kept in mind that in order to effectively counter phishing and quishing attacks, a multi-faceted defense strategy is essential. Relying solely on one method is insufficient. A collaborative approach, utilizing various lines of defense, is crucial for comprehensive protection against these threats. The user should always check the URL and the website before interacting with it. It is also recommended to use QR code apps which have advanced safety features incorporated, such as checking the URL against blacklisted phishing websites.

5 LIMITATIONS AND FUTURE WORK

This paper proposes an advanced approach to QR code security, integrating strategic design techniques to mitigate tampering risks. However, acknowledging our study's limitations is critical for a comprehensive understanding of its scope and impact.

As this research is a work in progress, we have not yet fully tested the extent to which the difficulty for an attacker to counterfeit a SafeQR code increases. While our design techniques are theorized to complicate the tampering process significantly, the lack of empirical evidence limits the assertion of their effectiveness. Future work should, therefore, include testing scenarios where attackers are challenged to fake SafeQR codes under various conditions, providing empirical data to validate the proposed designs' security benefits. Moreover, while our design strategies complicate the tampering of genuine posters, they cannot guarantee protection against attackers who might create completely fraudulent posters. The potential for such scenarios underscores the necessity for additional security layers, possibly in the digital domain, to authenticate the origin of physical posters.

The user study's design introduces a limitation, given that it was conducted in a public space without a controlled participant selection. The spontaneous nature of participant interaction, while valuable for real-world insights, does not allow for a controlled examination of demographic-specific responses or behaviors. Therefore, the results may not be entirely generalizable in other contexts.

This work is an initial exploration and should thus be considered a starting point for further research. The future trajectory of this project will include:

- Broadening the evaluation to include a larger, more diverse participant base, allowing for stronger statistical validity and insights that are more representative of the general population.
- Design and conduct controlled experiments to understand and validate the challenges an attacker would face when counterfeiting SafeQR codes.
- Investigating digital authentication methods that could work in tandem with our physical security features to address the limitations posed by completely fake posters.

6 CONCLUSION

In this paper we aimed to explore novel ways of protecting QR code users from quishing attacks by enhancing the integrity of QR codes through harnessing design for security. While much of the effort in QR code security is based on user education, this project leads towards simplifying the process for users to identify potential fraud and simultaneously making it much harder for Attackers to fake the printed QR code. We believe that the current situation where an attacker can tamper in little to no time with almost no effort and costs hundreds of QR codes, is one of the main reasons of quishing attacks being so common. The proposed defense strategies address this issue by significantly increasing the complexity and time required for tampering, thereby disrupting the ease and speed that make quishing attacks appealing to attackers while also making tampering more visible to users, enabling them to detect these attacks.

REFERENCES

[1] Ahmed Abbasi, David Dobolyi, Anthony Vance, and Fatemeh Mariam Zahedi. 2021. The Phishing Funnel Model: A Design Artifact to Predict User Susceptibility to Phishing Websites. *Information Systems Research* 32, 2 (2021), 410–436. https://doi.org/10.1287/isre.2020.0973

[2] bitly. 2024. Dynamic QR-codes advertised by QR-code creation websites. Retrieved January 17, 2024 from https://www.qr-code-generator.com/solutions/dynamic-url-qr-code/.

[3] European Union Agency for Cybersecurity (ENISA). 2023. *ENISA Threat Landscape 2023.* ENISA Threat Landscape. European Union Agency for Cybersecurity (ENISA). https://doi.org/10.2824/782573 Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (accessed on [2024-01-18]).

[4] Tobias Funke. 2024. QR code usage by country: Use-Cases around the world. https://www.qr-code-generator.com/blog/qr-code-usage-country/

[5] Brandon Gavett, Rui Zhao, Samantha John, Cara Bussell, Jennifer Roberts, and Chuan Yue. 2017. Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLOS ONE* 12 (02 2017), e0171620. https://doi.org/10.1371/journal.pone.0171620

[6] Katharina Krombholz, Peter Frühwirt, Peter Kieseberg, Ioannis Kapsalis, Markus Huber, and Edgar Weippl. 2014. *QR Code Security: A survey of attacks and challenges for usable security.* Springer, Vienna, Austria. 79–90 pages. https://doi.org/10.1007/978-3-319-07620-1_8

[7] Joseph B. Lyons, Charlene K. Stokes, Kevin J. Eschleman, Gene M. Alarcon, and Alexander J. Barelka. 2011. Trustworthiness and IT suspicion: An evaluation of the nomological network. *Human Factors* 53, 3 (5 2011), 219–229. https://doi.org/10.1177/0018720811406726

[8] Vasileios Mavroeidis and Mathew Nicho. 2017. Quick Response Code Secure: A Cryptographically Secure Anti-Phishing Tool for QR Code Attacks. In *Computer Network Security (Lecture Notes in Computer Science)*, Jacek Rak, John Bay, Igor Kotenko, Leonard Popyack, Victor Skormin, and Krzysztof Szczypiorski (Eds.). Springer International Publishing, Cham, 313–324. https://doi.org/10.1007/978-3-319-65127-9_25

[9] Federal Bureau of Investigation. 2022. Cybercriminals Tampering with QR Codes to Steal Victim Funds. Retrieved January 17, 2024 from https://www.ic3.gov/Media/Y2022/PSA220118.

[10] Heather Parker and Stephen Flowerday. 2020. Contributing factors to increased susceptibility to social media phishing attacks. *SA Journal of Information Management* 22 (06 2020). https://doi.org/10.4102/sajim.v22i1.1176

[11] Filipo Sharevski, Amy Devine, Emma Pieroni, and Peter Jachim. 2022. Gone Quishing: A Field Study of Phishing with Malicious QR Codes. arXiv:2204.04086 [cs.CR]

[12] SoSafe. 2022. What is QR Phishing? | Examples & Prevention Tips. https://sosafe-awareness.com/glossary/quishing/

[13] Arun Vishwanath, Brynne Harrison, and Yu Jie Ng. 2016. Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research* 45, 8 (2 2016), 1146–1166. https://doi.org/10.1177/0093650215627483

[14] WCNC. 2022. Where's The Money: Beware QR code scams. https://www.youtube.com/watch?v=4bQRoiNXVxk

A QR CODE POSTERS

Figure 5: All posters used in the second user study at the University. From left to right: (a) StandardQR tampered (b) StandardQR (c) SafeQR (d) SafeQR tampered