Exploring Phishing Threats through QR Codes in Naturalistic Settings

Filipo Sharevski
DePaul University
fsharevs@cdm.depaul.edu

Mattia Mossano
Karlsruhe Institute of Technology
mattia.mossano@kit.edu

Maxime Veit
Karlsruhe Institute of Technology
maxime.veit@kit.edu

Gunther Schiefer
Karlsruhe Institute of Technology
gunther.schiefer@kit.edu

Melanie Volkamer
Karlsruhe Institute of Technology
melanie.volkamer@kit.edu

***Abstract*—QR codes, designed for convenient access to links, have recently been appropriated as phishing attack vectors. As this type of phishing is relatively and many aspects of the threat in real conditions are unknown, we conducted a study in naturalistic settings (n=42) to explore how people behave around QR codes that might contain phishing links. We found that 28 (67%) of our participants opened the link embedded in the QR code without inspecting the URL for potential phishing cues. As a pretext, we used a poster that invited people to scan a QR code and contribute to a humanitarian aid. The choice of a pretext was persuasive enough that 22 (52%) of our participants indicated that it was the main reason why they scanned the QR code and accessed the embedded link in the first place. We used three link variants to test if people are able to spot a potential phishing threat associated with the poster's QR code (every participant scanned only one variant). In the variants where the link appeared legitimate or it was obfuscated by a link shortening service, only two out of 26 participants (8%) abandoned the URL when they saw the preview in the QR code scanner app. In the variant when the link explicitly contained the word "phish" in the domain name, this ratio rose to 7 out of 16 participants (44%). We use our findings to propose usable security interventions in QR code scanner apps intended to warn users about potentially phishing links.**

I. Introduction

Phishing attacks date back to the early days of the Internet [40] and are considered as one of the most lasting security threats, meant to either steal sensitive information (e.g., credentials [32]) or to deliver malicious payloads (e.g., ransomware [17]). The threat of phishing is hard to eradicate as attacks targeting credentials or delivering malware saw a 150% yearly increase since beginning of 2019 [3]. Researchers in academia and industry continuously propose new and updated solutions to curb phishing attacks, but attackers are still able to evade defenses tailored to known attack vectors or use novel ones [56], [57]. One such novel vector that is increasingly used for phishing purposes are *Quick Response (QR) codes* [18].

QR codes offer an easy way to deliver information that eliminates the need to directly type complex textual strings, such as identification numbers or links to websites (i.e., Universal Resource Locators or URLs) [47]. Despite this convenience, QR codes did not achieve widespread adoption for several years and were mainly seen as a potential future market [24]. The COVID-19 pandemic, though, brought about a new, unforeseen requirement for a contactless exchange of information, for which the QR codes were an ideal solution. What was once an optional tool became the go-to method for information transfer, adopted both in COVID-19 specific situations (e.g., test centers) and mundane ones (e.g., restaurant menus). The abrupt proliferation of QR codes opened up a new opportunity for attackers, because people are focused on completing their primary task without physical contact (e.g., accessing a link) rather than looking for cues of phishing in the link embedded in the QR code. For example, phishing QR codes were discovered in parking meters throughout San Antonio [4] and a backdoor in an open-source QR code generator was revealed embedding phishing links [31]. Since the pandemic the use of QR codes saw their resurgence from a state of near-extinction [22] to a continuous increase over the last few years that seems not to stop [44]. Hence, we must consider the potential threats that might accompany their use.

The threat of phishing through QR codes warrants equal attention as the traditional phishing through email, SMS or voice, for four reasons. First, current anti-phishing awareness measures rarely cover attack vectors outside of the traditional ones [30]. This leaves people unaware and ill-prepared to deal with attacks through QR codes. Second, people's attention is focused on successfully accessing the link behind the QR code while avoiding any inconvenience through the scanning process, disregarding potential phishing cues [10]. Third, while people could assess emails, SMS, or voice messages for phishing cues (e.g. sender's address/number, URL, or attachments), this is not the case for QR codes, which when scanned by a QR scanner app, mainly show the embedded link and nothing else. Fourth, to the point above, people lack the ability to spot a phishing attack just from the URLs themselves [1], [63].

As shown in [58] the majority of people don't inspect the URLs embedded in QR codes, while [45] shows that they even opt to use their single sign-on credentials (e.g., Facebook or Google) to sign-up for a convenience service. But this last evidence was obtained for URLs leading to online

Symposium on Usable Security and Privacy (USEC) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-5-2
https://dx.doi.org/10.14722/usec.2024.23050
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

surveys and used either a "social study" or a "COVID-19" pretexts, leaving the question of how people naturally behave around QR codes in physical spaces and use pretexts also used in ongoing, real-world traditional phishing attacks. Studying how people are naturally exposed to the threat of QR code phishing, albeit on the surface similar to regular phishing, requires the consideration of unique factors outside of the online environment, for example, observing differences in how people interact with links sent over email versus links accessed by scanning a QR code [47].

While an online environment naturally fits an email phishing study, QR codes are usually found in physical, public spaces, such as restaurants, cafeterias, or train stations. Thus, it is required to observe how people interact with potentially phishing QR codes in a physical environment. This requires a non-trivial study setup, because researchers have first to allow for people to be naturally drawn to a QR code, observe their brief interaction from a distance (to avoid "tipping them off" that something is amiss with the QR code), and then approach each individual person immediately to get their first account impressions of the interaction.

We took upon this challenge and conducted an observational study in a metropolitan area in the US to explore how people face phishing threats through QR codes in naturalistic settings. We deem the action of opening the embedded link in the QR code without inspecting the link for potential phishing cues as an exposure to a "phishing threat" because: (1) once the URL is loaded in the browser people might spot a credential harvesting page but cannot protect themselves from a malware designed to automatically install on their phones; and (2) the naturalistic settings preclude doing any actual phishing (also such a study would not have been approved by our Institutional Review Board as it would have exposed participants to a greater than minimal risk, e.g., reveal their real credentials).

We created three large color posters that included a QR code placed in a humanitarian message in reference to the ongoing conflict in Ukraine. We chose this particular humanitarian pretext because around the time we conducted the study, there were reports of real-life phishing attacks with the same pretext [29], [48]. The QR code in each poster embedded a distinct link variant: (i) a *legitimate URL*, (ii) an *explicitly-phishing URL*, or (iii) a short URL service that redirected to an *implicitly-phishing URL* (each participant scanned only one link). The purpose of this variation was to observe if people actually inspected the URLs for possible phishing cues, for example explicitly using the word "phish" in the domain name or using URL shortening services, a common attacker trick.

Here, we note that real-world phishing links rarely include an explicit cue such as "phish" in their domain names. Yet, our objective was not to test the limits of the link deceptiveness but rather how people act to a phishing threat associated with obviously deceiving and untrustworthy domain names. The posters were placed unattended in three areas with high pedestrian traffic, such as malls, cafes, and cultural points of interest. We as researchers, were unassumingly positioned in the near vicinity of the poster to observe anyone that scanned the QR code. Once we noticed this, we approached them and conducted a brief interview about the encounter with our poster and their general experiences with QR codes.

Our results show that 67% of the people that decided to scan the QR code opened it in their browser without inspecting it for possible phishing cues (i.e., unwittingly exposing themselves to a phishing threat). The salience of pretext topic played a major role into attracting participants, with 52% of them scanning the QR code for this reason alone. Per URL type, one participant in the *legitimate URL* group, 7 in the *explicitly-phishing URL*, and one in the *implicitly-phishing URL* group were suspicious enough to abandon the link when seeing the preview in their QR code scanner app. On a related note, 19% of our participants explicitly pointed to inefficiencies of the QR code scanner app interface as the reason why they did not inspected any of the URLs in our study. Our results suggest that addressing the current insecure behavior of people lays not only in raising awareness, but also in developing usable security indicators within the QR code scanner apps to warn users about potentially phishing QR codes.

Scope and contribution of this work. With this work we produced evidence related to the behavior in naturalistic settings where a person might open a potentially phishing link embedded in a QR code without inspecting for potential phishing cues. Our research questions are detailed in Section III-B, in response to which we produced these main contributions:

- Evaluation of the participants' exposure to QR code phishing threats in naturalistic settings;
- Evidence that the choice of a pretext is a major factor for an exposure to potential phishing threat through a QR code as an attack vector;
- Evidence of users' ill-preparedness to deal with naturalistic QR code phishing threats and the necessity of awareness measures;
- Proposal of actionable countermeasures and design recommendations for a QR code scanner app to warn users about potentially phishing links embedded in QR codes.

Following the introduction, we summarized the known phishing threats through QR codes in Section II. We then described our study design, the pretext and the phishing tactics we chose, and the measurements we employed to capture participant behavior in Section III. Section IV contains our study results. The findings are discussed in Section V where we outline a usable security proposal for QR code scanner app interfaces to warn people about potentially phishing links ahead. Finally, we offer our conclusions in Section VI.

II. Background Research

A. Traditional Vs. QR Code Phishing

Phishing, the fraudulent attempt to obtain sensitive information by disguising oneself as a trustworthy entity, is a perennial security threat, as attacks breach security protections (e.g., authentication) usually with the goal to obtain unauthorized access to sensitive data [23]. The unique feature of phishing is that the target of the attack is not a system or a technology *per se*, but the people who use these systems and technologies. As such, anti-phishing solutions abundantly focused on improving users' awareness [39]) implementing usable detection cues [20], and filtering out phishing content [60]. This anti-phishing effort considers emails to be the most convenient phishing vectors, be that because of easiness for impersonation [49],

easy-to-implement phishing tricks [54], and the continuous ability to evade phishing filters [8].

Other phishing vectors, albeit on a much smaller scale, have been also used in successful attacks, for example SMS texts and voice calls [56]. Both of these vectors, similar to the email, have exploited vulnerabilities in human behavior (e.g., persuasion principles like authority, scarcity, reciprocity, or social proof [19]), lack of awareness (e.g., unknown senders/callers, or content/format check), and filtering on the side of the text/voice provider. A new vector, different than these traditional ones, recently appeared on the phishing landscape – QR codes. Phishing QR codes, as shown in Table I, require a less elaborate set up, as attackers need only to embed a phishing link in a simple QR code and distribute it either in a physical space (e.g. stickers, or posters) or over email/message (QR codes are not yet considered as suspicious elements for filtering [10]). While the QR code vectors could well use the traditional susceptibility factors (e.g., reciprocity or scarcity/urgency to complete a payment), they also introduce another factor – *immediacy* – where users are focused on the immediate access to a service or the quick completion of an action (e.g., opening a restaurant menu or giving a donation).

While for the traditional attack vectors there are plenty of usable detection cues, such as phishing email warnings [55], URL highlighting [60], or caller IDs (e.g. Scam Likely), QR code users have no such indicators at their disposal as the standard QR scanner apps square and present any link – phishing or otherwise – in the same manner. The traditional phishing vectors face an increasingly difficult task of adaption to the advanced detection and filtering performed on the side of the email or phone providers, but no such thing exist for the QR codes as vectors as there is no intermediary between the people and the links embedded in these QR codes. Lastly, there is abundant training and awareness opportunities for individuals to learn how to spot and avoid email, SMS or voice phishing attacks [61], but no such training or awareness is available for phishing attacks through QR codes.

B. QR Code Phishing in Practice

Phishing attacks using QR codes as vectors, so far, either "worked" because people were curious to see what was behind the QR code [28], or expected a personal benefit in return [45], [58]. However, in both cases, the attacks were simulated (e.g., no actual credential harvesting happened) and the evidence for the potential phishing success was collected in controlled or laboratory settings (e.g., solicited on college campuses or via survey delivery of a QR code). Because QR codes entail a *physical* interaction that precedes the actual act of accessing a link, a more adequate approach for investigating potential exposure to a phishing threat is to observe how people interact with QR codes in naturalistic settings. An effort to capture the natural behavior around regular, non-phishing QR codes was made in [58] using an unassuming surveillance CCTV camera that recorded people's unwitting interaction. The findings indicate that 85% of the participants scanned and opened the embedded URL in the QR code without inspecting it. Yet these findings provide limited evidence of the *actual* behavior of ordinary people because the location of the QR code was in a computer science building, capturing a relatively small and technologically-sophisticated population.

Phishing attacks through QR codes might continue to "work" because people have scarce assistance in spotting phishing QR codes. A verifiable infrastructure to ensure the QR code URL authenticity, as proposed in [28], is inherently restrictive as it doesn't preclude people from abandoning a complex QR scanning system in favor of a simple one. Another possibility lies in implementing warnings to "nudge" people to scan only QR codes with distinctive properties (e.g. logos), as proposed in [26], but it is increasingly trivial for attackers to impersonate such codes. Studies of QR phishing awareness training, such as the one proposed in [45], to our knowledge, have yet to find their way into mainstream awareness efforts, leaving people without actionable tools on how to identify QR codes containing malicious phishing links.

III. Study: Phishing QR Codes

A. Naturalistic Settings and Baseline Behavior

When we refer to naturalistic settings, we consider the definition of Robinson et al. [42]: the circumstances where a person unassumingly encounters a QR code and independently chooses to scan and access the embedded URL. A baseline safe behavior in these naturalistic circumstances would be for the person to inspect the embedded URL in the QR code while it is showing in the QR code scanner app for potential phishing cues *before* it opens the link in a browser (the baseline behavior of the QR code scanner app displays a preview of the URL in a highlighted square surrounding the QR code on which the user needs to *explicitly* tap or give a voice command in order to open the embedded link in the browser on their phone).

These cues could range from suspicious domains names, typos, misspellings, or URL shortenings that are implemented to deceive users by impersonating a legitimate-appearing URL – a regular, non-phishing URL (e.g., mail.google.com vs. mail.gooogle.com – where an additional letter "o" is added in the domain name [41]). A deviation of this baseline behavior towards facing a potential "phishing threat" from a QR code would be for a person *not to inspect* the URL in the QR code scanner app, but instead proceed to open it in their browser without looking for possible phishing indicators. One could argue that browsers' blocklists might prevent a suspicious URL to be loaded in the first place [**?**], but these blocklists cannot stop unreported phishing URLs and in this cases people still need to inspect the URLs themselves.

This leaves the possibility for a person to inspect the URL in their browser, spot a credential harvesting page, realize that something is amiss, and abandon the link. However, past evidence shows that many users don't inspect URLs coming from emails or messages at all and simply enter their credentials into the associated website [5], [27]. The inspection of the URL in the browser, additionally, might come too late, because the mere loading might have already triggered an automatic installation of malware designed to steal credentials or install spyware, as evidence from the real-world phishing shows [11]. So, any deviation from the action of inspecting the embedded URL in the QR code *before* opening it in a browser constitutes an exposure to a phishing threat in naturalistic settings associated with a QR code.

TABLE I: Comparison between Traditional (Email, SMS, Voice) and QR codes as Phishing Vectors

Feature	Traditional (Email, SMS, Voice)	QR codes
Attacker Planning	Mass distribution or spear-phishing	Physical spaces and/or sharing it over email/message
Attacker Execution	Sender spoofing, intentional errors in formatting (to evade detection/filtering), creation of malicious links/webpages and attachments containing malware	Embedding a link in a QR code, posting it in
Susceptibility Factors	Authority, scarcity/urgency, reciprocity, liking, social proof, information overload	Immediacy (e.g. the need to access a service or complete an action)
System-side Defenses	Mail/phone provider detection filtering (e.g. spam detection, phone number denylist), browser-based URL filtering	Only browser-based URL filtering
User Interface Defenses	Mail/phone client or application warnings (e.g. phishing alerts, URL highlighting, "Scam Likely")	No indicators of deception in QR code scanners
User Preparedness	Phishing and spam training and awareness	None

B. Research Questions

The recent use of QR codes as phishing vectors has revealed a gap in our understanding of how people behave when exposed to phishing threat through QR codes in naturalistic settings because the interaction is brief, driven towards *immediate* convenience in completing tasks (e.g. accessing menus, payment, ticketing, etc.), and requires a physical presence for observation. To address this gap, we designed an observational study to explore the following research questions:

- **RQ1**: What factors attract and persuade people to access an URL embedded in a QR code in naturalistic settings?
- **RQ2:** What actions do people take when accessing an URL embedded in a QR code in naturalistic settings?
- **RQ3**: What kinds of experiences people have with suspicious QR codes they encountered in naturalistic settings?

C. Pretext and Infrastructure

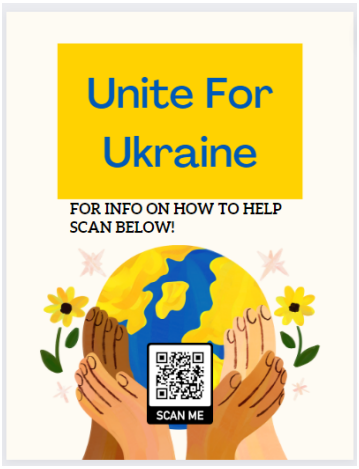
The pretext in our study employed several elements that are characteristic of both standard phishing campaigns and of past QR phishing studies done in controlled laboratory settings. We chose to use a poster, shown in Figure 1a, printed in color in size 36 x 48 inches, with a 8 x 8 inches QR code. The topic of the poster was humanitarian and it was chosen to resonate with similar pretexts used in real-world phishing attacks circulating at the time of the study [29], [48]. The poster invited people to scan the QR code in order to obtain more information on how to help Ukrainians affected by the conflict, including a photo of a diverse set of hands holding a globe (hinting to solidarity to leverage the *social proof* persuasion principle of phishing [19]) along with blue and yellow text (alluding to the colors of the Ukrainian flag). Similar humanitarian campaigns for helping the people of Ukraine were already underway around the US [21], so it was fairly reasonable for people to believe that the poster provided an opportunity for them to offer their help.

The QR code, framed in a box that stated "scan me," as shown in Figure 1a, embedded one of three different links: (1) a *legitimate looking URL* or https://supportukranianconflict.com/; (2) an *explicitly-phishing URL* or https://phishmeforukraine.com/; and (3) an *implicitly-phishing URL* or https://tinyurl.com/ that redirected to https://unclesamsupportsukraine.com/. We deliberately choose to use unknown domains for our URLs because an impersonation of a trusted/known domain might have been blocked before the end of the study, making the comparison difficult. Equally, we might have run into copyright or other types of property infringement of the original owners of the URLs, causing greater than a minimal harm to them (a stipulation of minimal harm to anyone involved in our study was required for the approval by our Institutional Review Board). For the same reason, we also decided not to impersonate an actual humanitarian organization to avoid causing more than minimal harm both to the participants and the organization.

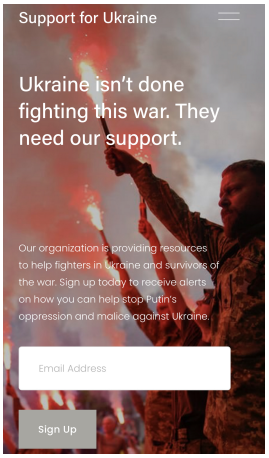
In the *explicit-phishing URL* variant, we wanted to see if people recognized an explicit cue when the word "phish" was included in the domain name of the URL, which was not present in the *legitimate looking URL* variant. We were aware that real-world phishing links rarely include an explicit cues such as "phish" in their domain names, as this would defeat the essential purpose of these attacks. However our objective was not to test the limits of the link deceptiveness, but rather how people react to a phishing threat associated with obviously deceiving and untrustworthy domain names that are embedded in QR codes. In other words, our objective was to learn if the *immediacy* of the QR code is sufficiently potent to make people ignore even overt cues of phishing deceptions.

In the *implicitly-phishing URL* variant we wanted to see if an obfuscated URL with a fairly known service for URL shortening (i.e. "tinyurl") would raise alarms about potential deception ahead that leads to suspicious looking URL. Here too, we were aware that real-world phishing attacks that use URL shortening rarely lead to colloquially worded domain names. Yet, as in the explicit case, our objective here was to see if people would inspect the redirected URL to see if something is amiss with the overall QR code setup. Of particular interest was observing the decision-making behind accessing these potentially suspicious links, so we choose to use secure URLs and to create a realistic scenario where the security indicators employed by standard smartphone browsers (e.g. padlocks) are present as part of the overall phishing pretext.

All of the URLs led to a same landing page, shown in Figure 1b, which employed a minimal yet salient visual design



(a) Phishing Poster (legitimate QR code)



(b) Landing Page

Fig. 1: Phishing with QR codes: Infrastructure

which highlighted the sign-up options. We used a visceral image of Ukrainian soldiers holding stark red flares with superimposed text that stated the goal of the alleged organization was in providing humanitarian support to Ukraine, offering the option for people to sign-up with their emails. Our IRB approved the study up to the sign-up point, but we were not allowed to collect people's actual emails, so to avoid greater than minimal privacy risk. Therefore, clicking the sign-up button had no functional effect (i.e., the email field did nothing – no email was collected). Past studies redirected individuals from the login pages to a survey page [45], but we did not want to interrupt the flow of interaction of our participants. Hence, we chose to approach them once they finished with the mock sign-up and ask for a brief interview regarding their recent experience with the QR code they scanned (informing them explicitly that we did not collect their email or anything else that was entered in the sign-up form).

D. Data Collection Process

Our methodology for data collection employed several steps. First, we decided to conduct the study in a metropolitan area in the US and place the posters in areas with high pedestrian traffic, such as malls, cafes, and cultural points of interest. We obtained a prior approval to do so by both the authorities and the owners of these places, and we placed our posters next to other posters to blend with the naturalistic setting where such calls for humanitarian help, civic participation, or donation are regularly posted. To obtain approval, we fully disclosed to both the authorities and the owners of these places that we are conducting an anonymous study about potential phishing threats associated with QR codes, but that no actual phishing would have taken place, i.e., that both the poster and the embedded links were safe. The posters were incorporated in the environment so that passersby were naturally drawn to them in the course of their everyday activities. We, as researchers, were unassumingly positioned in the near vicinity of the poster to observe anyone that scanned the QR code. The posters were taken down and put back up every day during the data collection with the researchers present. This was done to avoid a situation where someone might scan the poster but is not offered the opportunity for participation or debriefed about the nature of the poster and the study overall.

Once we noticed this, we approached the potential participants, introduced ourselves as researchers, notified them that we noticed they scanned the QR code, and first asked them if they are 18 years of age or above to ensure their eligibility for the study. We didn't encountered anyone that was 18 years or younger, but we were nonetheless prepared to debrief them regardless of the ineligibility for the study (see bellow for more details on the debriefing process). We read a verbal script to our participants after their initial interested to participate in the study and the age check, shown in the Appendix, to obtain a verbal consent for their participation. We didn't encountered any participants that refused to participate (in that case we would have also debriefed them too).

After obtaining their verbal consent, we notified them that we did not collected any of the sign-up information they might have entered when they scanned the QR code. Next, we conducted a brief interview about the encounter with our poster and their general experiences with QR codes. The interview script, shown in the Appendix, was anonymous, and allowed participants to abandon the interview at any point or skip any question they were uncomfortable answering. The breakdown of interviews across days and locations in also given in the Appendix. The interview was recorded on a portable voice recorder, and participants were notified that the recording would have been transcribed in a second time for analysis purposes. We also warned the participants to refrain from stating any personally identifiable information during the interview – we would have removed it during the transcription, but anyhow there would have been a brief period where their anonymity would have been appended, so we wanted to avoid that situation. We obtained an approval from the IRB stipulating participants to be at least 18 years old and familiar with QR codes. Each interview took around 8-10 minutes. The participation was voluntary but we nonetheless offered our participants free candy as a compensation for their time.

As our study was approved as a non-full disclosure protocol, we employed a lengthy debriefing process with each participants after we concluded the interview. First we ensured that there was no harm caused to participants and told them that we put the poster and we controlled the URL behind it. We told them that even if the sign-up page had an input field for an email, the input field did nothing when they clicked "sign up" meaning that we did not collect their email or that there is no risk of privacy invasion as the submit event did not sent their email back to the hosting server not their email was stored anywhere. Next, we showed participants the evidence of the current real-world phishing campaigns using the humanitarian pretext for the conflict in Ukraine and explained that we used the same pretext to observe a similar phishing threat associated with the QR code they just scanned [29], [48], [33].

We ensured the participants that the use of the pretext was not disrespectful to the Ukrainian people but worked towards raising the awareness about the dangers of phishing, that could ultimately undermine the humanitarian help – an outcome we as researchers worked to prevent through the publication of our study. Here, we pointed participant to legitimate humanitarian organizations operating in Ukraine where they could contribute to on their own (e.g., UNICEF or Amnesty International [53], [2]). We also pointed our participant to resources about raising general phishing awareness regardless of the phishing vector and shared our contact if they wanted to contact us in case they encountered any suspicious URL in future. At the end of the debriefing process, we offered them the option to ask for their data to be removed after their participation (no one did so, and we were prepared to delete the interview recording with the participant present to ensure we removed their data).

E. Pilot Study

Since this was, to the best of our knowledge, the first study concerning phishing threats through QR codes in naturalistic settings, we decided to perform a pilot study with a smaller amount of participants before we commenced with a larger study sample. We did so in order to verify the pretext, to test-run the poster placement and the approach, to test the interview script and workflow, and debug the overall process of data collection and analysis. We used the same research setup as detailed above, including the poster placement, the verification of age and eligibility, the obtaining of the verbal consent, and the lengthy debriefing process. For the pilot study, we ended with 18 participants (six per URL type), sufficient to cover all the data collection places and to gather the initial behavior around each of the study URLs. The pilot phase lasted 2 weeks and we ran it at the beginning of 2023. All participants, except one in the *explicit-phishing URL* group, did not inspect the URLs for phishing cues. The only one that did, reasoned:

> "*I was suspicious when my phone read the URL as https://phishmeforukraine.com/; Did not trust the site after that; Not about to give any information for a site with a URL that starts with "phish", unless it is for the band.*"

Most of the participants were attracted to the pretext, indicating that the topic was well selected and relevant to the target population of a metropolitan area in the US in early 2023. Following the pilot study, we commenced the data collection of the main study. The main data collection lasted for six weeks in the first half of 2023 and we collected 42 participants responses. We interviewed anyone who scanned to code (i.e., that interacted with the poster), meaning that there were no participants during our observations that were not approached. Due to the naturalistic essence of the study itself, no formal invitation to participate was possible. However, we offered whoever scanned our QR code the option to be removed from our dataset and not proceed with the interview. No one took this option. We conducted a brief analysis to check and confirm that we have reached a saturation so we decided to conclude the data collection and start with an in-depth analysis of the interview responses.

F. Data Analysis Process

Our data analysis process also involved several steps. We started with an inductive coding approach (as described in [43] and [52]) as to identify frequent, dominant or significant aspects in the answers of our participants. One of the researchers open coded all the interviews. The resulting codes were then discussed with a second coder, who then independently coded all the interviews. After the first round of coding, we calculated the *Inter-Rater Reliability* (henceforth, *IRR*) using Cohen's kappa [13] to determine the level of agreement of the two coders. The initial IRR was $k = 0.58$, which we deemed insufficient to be acceptable.

A new phase of discussion followed the first cycle of coding to solve the conflicts in the coding whenever they appeared. We then restructured the codebook to represent the new understanding reached, and both coders independently coded the material again. We re-calculated the IRR again, reaching a Cohen's kappa of $k = 0.90$, which we deemed acceptable. The open codes were then used to structure a hierarchical codebook to capture the three main aspects identified: (i) *delivery vector*, i.e., codes pertaining to the vector used to deliver the phishing attack; (ii) *website vector*, i.e., codes related to the website targeted by the QR code and the participants' behavior around it; and (iii) *behavior*, i.e., codes describing the participants' everyday interactions with QR codes. The full codebook is available in the Appendix.

IV. Results

This section presents the demographic make up of our sample as well as all of our findings per each research question of the study. For brevity, we included only the most frequent and important codes yielded from our data analysis and interpretation, with the full breakdown of the codes for each research question provided in the Appendix. Note, not all participants answered all interview questions, therefore some of the reported numbers and percentages might not amount to 100% of the sample when capturing a particular aspect of people's behavior. Note further that codes not related to a particular research question are sometimes present in the calculations shown in the figures. This is because participants sometimes mentioned aspects of interest for one research question in an answer related to a different research question. For example, while answering if they visited the website after scanning the QR code (RQ2), a participant might have mentioned being interested in the topic (RQ1). We also included a breakdown of the results per the type of URL seen by the participants

for completeness. For a richer presentation of our findings, we also included verbatim quotations from participants, wherever appropriate, to capture their natural interaction with the posters and QR codes overall after scanning them.

A. Demographics

A total of 42 people interacted with the posters, none of whom declined to participate. Our participants were 38% female and 62% male. The majority had college education (64%), followed by post graduates (21%), high school degree (7%) and unspecified degree (8%). Age-wise, 29% were in the [25-34] group, 24% in [18-24], 24% in [35-44], 17% in [45-54], 4% in [55-64], and 2% in [65+]. Relative to QR codes proficiency, 52% reported it as "high," 43% "intermediate," and 5% "low." As this was a study in naturalistic settings, we could not control the type of devices nor the QR code scanner app used to scan the QR code, therefore we collected this information as well. 82% of our participants used Apple iPhones, 12% had a Samsung Galaxy (i.e., an Android smartphone) and 6% declined to release this information. This is a typical distribution of smartphone devices in the US i.e. where the study took place [14]. All participants used the standard QR code scanner app included in iOS and Android OS – 64% used Safari and 36% Google Chrome to open the links.

B. RQ1 - Pretext Persuasion Factors

The results of our first research questions, summarized per the most frequent codes, are shown in Table II. Note, the total number of codes exceeds the number of participants because each answer contained one or multiple codes, i.e. they mentioned more than one factor. The most attractive factor that persuaded our participants to approach the poster and scan the QR code was the humanitarian aid topic. Many participants stated that they were attracted to the poster to "*add [their] support to the Ukrainian people*," with some noting that the "*poster looked harmless*," "*friendly*," and "*unassuming*." The features of the poster themselves were also considered attractive and persuasive, such as the color scheme, the text of the poster's message, and the poster's size. For example, one of the participants stated that the poster's "*vibrant colors*" attracted them, and another pointed that they were drawn by the "*bold title 'Unite for Ukraine'*".

The geopolitical context of the poster was also noted as a factor that attracted our participants and persuaded them to scan the QR code. Here, one participant justified their interaction with the poster in these words: "*I'm not interested in scanning QR codes very much, [but] this one stood out, since I heard the war is actually past its one year mark*." General curiosity was also tied to the pretext, as participants explained they were "*drawn by the location of the poster in the coffee shop*" or scanned the QR code because they were "*just bored waiting for [their] girlfriend*" in a mall. One participant said they were curious to see more about a "*poster and a QR code that could not be missed from a mile away*."

TABLE II: RQ1: Pretext Persuasion Factors

Code	Found	Percent of total
Poster's topic (humanitarian aid)	22	52%
Poster's color	10	24%
Poster's text	7	17%
Poster's size	4	10%
Poster's geopolitical context	4	10%
General curiosity	3	7%

C. RQ2 - Actions Around QR Codes

1) General Actions: The results of our second research questions, summarized per the most frequent codes, are shown in Table III. Here too, the total number of codes exceeds the number of participants because each answer contained one or multiple codes, i.e., actions. With respect to actions taken to determine the legitimacy of a QR code's embedded URL and the associated website, most of the participants opened the URLs in their browsers without inspecting the URL for phishing (or any other) cues. These participants stated that they "*didn't pay attention to anything particular*" because they were focused to find out "*how they can assist the people affected in the Ukrainian conflict*". The second most frequent action that our participants did was to inspect the URL for phishing cues, but only after they scanned it and opened it in the browser. One participant stated that they "*looked at the URL and it said 'Ukraine' so they were OK with it*".

The third most frequent action our participants performed was to inspect the general look of the landing page shown in Figure 1b, but not the URL. These participants noted that they "*read the blurb and thought it was safe to use, the website looked OK*" or "*specifically payed attention to the people holding the flares*." The fourth action that participants in our study took was to inspect the URL in the QR code scanner app. These participants stated they "*look at the URL before [they] open it in a browser just to make sure it isn't something odd*". They also said they "*looked at the URL and it said 'Ukraine' so they were OK with it*." Only 7 of the participants exhibited the baseline behavior in the case of the *explicit-phishing URL* variant i.e. they decided not to open the URLs in their browser "*cause [they] saw the word 'phish'*" when the QR code scanner app displayed the domain name.

Interestingly, an equal number of participants specifically pointed to the inefficient interface of their QR code scanner app as the reason behind them not checking the URL in it. For example, one participant stated that "*the URL disappeared so [they] tried to investigate but it was too late*." Another, also keen on inspecting URLs, pointed out that they have to do it "*once [they are] in the browser, because when the URL is highlighted yellow [they are] usually more focused on whether the QR code is working in the first place*." There were also participants that were concerned with both the QR code scanner display of the domain name, the URL in the browser, and the landing page, expressing that in the case of the *implicit-phishing URL* "*the QR code was concerning, 'phish' or something like that, so was the redirected URL and the website had a different address*".

2) Actions Per URL Type: We specifically varied the URL domain name to explore how people deviate from the baseline secure QR code scanning behavior and whether they will: (i) be suspicious of an otherwise legitimate looking URL; (ii) be suspicious of an explicit cue with the word "phish" in the URL; and (iii) become suspicious of an implicit cue from an obfuscated URL with a known service for URL shortening.

TABLE III: RQ2: Actions Around QR Codes

Code	Found	Percent of total
URL clicked and accessed without inspection	28	67%
URL inspected for phishing cues	15	36%
URL no inspected but website's general look inspected	13	31%
URL inspected for phishing cues in the QR scanner App	9	21%
Url not inspected due to inefficient QR scanner interface	7	17%

Our findings are summarized per URL type and per interview codes in Figure 2. Each participant accessed only one type of URL, with the following breakdown: 11 – legitimate URL, 16 – explicitly-phishing URL, and 15 – implicitly-phishing URL. We aimed to balance the distribution as equally as possible, but we could not completely control how many people scanned each the QR codes in each variant due to the nature of the study.

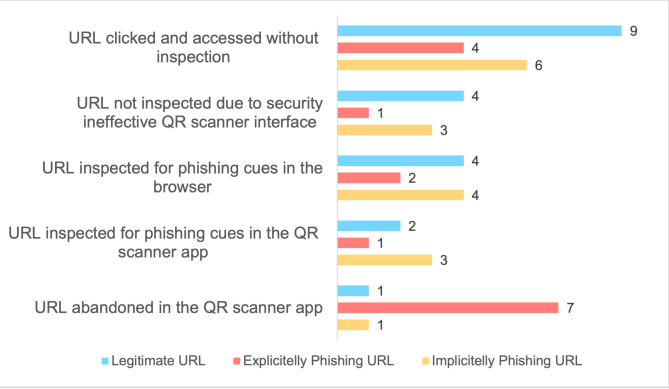


Fig. 2: RQ2: Actions Around QR Codes: Per URL Type

In the first scenario, nine of the participants opened the *legitimate looking URL* – the regular, non-phishing URL – in their browser without inspecting it in the QR code scanner app. Four did so due to the security ineffective interface complaining that it is "*hard to see the entire URL on [their] mobile browser, so [they] usually don't look into it but open it straight away*." Four of the participants in this group said they did inspect the URL once it was open and they saw the full webpage. Although two participants indicated they inspected the URL in the QR code scanner app and before they opened it, only one of them abandoned their scan or stopped, stating that they simply "*changed [their] mind on proceeding*."

In the second scenario, nine of the participants that scanned the *explicitly-phishing URL* decided to open it in their browsers without inspecting it. Six participants stated they inspected the link in their browser. Seven of the participants in this group, sensing something was amiss, decided not to open the URL after spotting the word "phish" in the URL when displayed in the QR code scanner app, noting that it was "*definitely a red flag*" for them as the link"*appeared to be malicious*." Four or the participants in this group stated they inspected the URL in the QR code scanner app but half of them anyhow opened the link in their browser. There was only one participant that pointed to the security ineffective QR code scanner app interface as the reason why they were not able to spot the obvious phishing cue early.

In the third scenario, eleven participants that scanned the *implicitly-phishing URL* opened it in their browsers. Nine participants stated they inspected the link *after* they opened it in their browser. The URL shortening service and redirection were not a red flag for most of them, though there was one participant that said they "*thought about abandoning it because I am familiar with the dangers of tiny URL*" (but nonetheless proceeded with the link). Although three participants in this group inspected the link in the QR code scanner app before opening it, none of them noticed that something was amiss, stating they "*looked at the URL before [they] opened it in a browser just to make sure it isn't something odd*." Three participantspointed to a security ineffective QR scanner app interface as the reason why they might have not been able to spot the URL redirection as a possible phishing cue. The one participant that decided not to open the link in their browser reasoned: "*I didn't follow through with the process as the link didn't look right to me; What if my phone would gets bricked? That's never a good thing.*"

D. RQ3 - Interaction with Suspicious QR Codes

The results of our third research questions, summarized per the most frequent codes, are shown in Table IV. Note, the total number of codes is smaller than the number of participants because not all the participants answered this question, i.e., two participants skipped this question. Regarding the general experiences of participants with QR codes, most of them stated that they have never noticed any suspicious interaction when dealing with QR codes relative to phishing or unusual behavior of the code. Mainly, participants were not aware of any possible problems with QR codes outside of the basic scanning functionality. Thirteen participants declared that they did encounter suspicious interactions but not very often "*because [they] really don't scan QR codes that often*." Three of our participants did encounter suspicious interactions with incorrect or non-intuitive formatting of the URL, which in turn "*threw [them] off, so they stopped*" after the scan and did not open the embedded link in their browsers.

TABLE IV: RQ3: Interaction with Suspicious QR Codes

Code	Found	Percent of total
Suspicious phishing interaction - No	24	57%
Suspicious phishing interaction - Not often	13	31%
Suspicious phishing interaction - Yes	3	8%

V. Discussion

A. Naturalistic QR Code Phishing

Our results suggest that studying exposure to the phishing threat through QR codes as attack vector is as informative and revealing in naturalistic settings as it was in controlled laboratory settings [28], [45]. Our participants were curious to see what was behind the QR code, namely because they were drawn to a pretext topic of humanitarian interest. Phishing threats need to be "believable" to the victims to work and materialize as attacks, i.e., sophisticated enough to be (i) *real*, (ii) *relevant*, and (iii) *persuasive* [25].

In term of realism, QR codes as phishing vectors do not need to worry much about spelling and grammatical mistakes in the pretext, because there is no filtering as a protection between the unwitting individuals and a phishing QR code (i.e., the attacker need not to craft a grammatically awkward text to circumvent automated detection). The same holds true for the sender's name and email address (or phone number), as a QR code pretext can simply look "trustworthy" without the need to spoof anything [34]. That is what we did with our poster, which read "United for Ukraine" and simply offered more "info" behind the QR code as a realistic, legitimate effort to help use the persuasive message of humanitarian aid. Another factor that influenced the trustworthiness of the poster was the choice of a realistic and accurate visual design. In our case, and unlike in email phishing [51], [62], we did not need to fabricate logos or fake any design copyright, but simply used a blue/yellow color scheme and a generic call to action to create an attractive and persuasive pretext.

In terms of relevance, traditional phishing attackers essentially rely on a believable email by selecting its context and premise to align with the target's environment, interests, and mental model [7]. While attackers have to infer the professional context of the victim when crafting an email (e.g., which other emails are usually sent to the victim), they need not to go into as much detail when using QR codes as attack vectors, as long as the pretext is of general interest among the target population. Hence, we selected a topic which resonates with the sentiment prevalent among people in the US [37], where our target population was. While inaccurate mental models of phishing make people ignore suspicious cues by highlighting relevant, yet deceptive, cues [6], no such models exists for phishing QR codes, explaining why a poster with a relevant topic had such a strong appeal to our participants.

In terms of persuasiveness, phishing emails often attempt to exploit the cognitive vulnerabilities in the people decision-making processes (e.g., heuristics, biases, and bounded rationality). While emails usually have to combine two or more persuasive principles (e.g., Cialdini [12]'s dimensions of authority, liking, scarcity, consistency, social proof and reciprocity), QR codes could simply use only one or add the *immediacy* to pique the curiosity of potential victims. We did so by selecting the "social proof" principle in addition to the immediacy, unlike the practice of using "authority" or "scarcity" as the principles that work the best for traditional phishing attacks [46].

Past studies in naturalistic settings indicated that 85% of a technologically sophisticated population was drawn to non-phishing QR codes [58]. In our case, we sampled a population that was fairly balanced between those highly and moderately proficient in QR codes and that used QR codes mainly for services such as restaurant menus or groceries. We also deliberately avoided placing the poster on or near a university campus, as past studies have done before, to get a more representative sample. Here, it is worth mentioning that the study reported in [58] was done in 2013 and we conducted our study ten years later – a period over which the QR code have become insreadingly popular and prevalent among people. If we consider the *legitimate URL* group to be on par with the event of scanning regular, non-phishing QR codes as done in [58], then we get a comparable result of 82% people drawn. We weren't approved by our IRB to actually "phish" our participants, but we found that at least 50% of the participants across all the URL variants did not inspect the link embedded in the QR code before opening it in their browser. This percentage is significantly above the 21% of the participants that behave similarly when tested for traditional phishing attacks in naturalistic settings [49].

The prospect of exposure to phishing treat associated with QR codes, even if conditional (i.e., the participants were not actually phished for their credentials or malicious software installed on their phones), seems alarming for both people as victims and QR code scanner app developers to take protective actions. The crucial event for reducing a potential susceptibility to a successful attack, at least for now, is the decision to open or not to open the embedded link in the QR code. This because people in naturalistic settings cannot rely on any phishing cue outside of those within the URL itself. However, the insufficient interface (i.e., QR code scanner apps that don't display the full path of the embedded URL) between the people themselves and the prospect of phishing victimization was explicitly pointed out by 19% of the participants across all URL variants, as they objected to the lack of an opportunity to closely inspect the URL before opening it.

Without a robust filtering (available as a default part phishing defenses), people are left to extrapolate from their past experiences or phishing awareness about phishing cues. We found evidence of this behavior in our study, as participants in all URL variants inspected the URL only *after* opening it in the browser of their smartphone. This result suggest that people are capable of looking for phishing cues, especially when a URL shortening service is used (as this is naturally suspicious, even if a shortened URL is shown in the QR scanner app), perhaps as a result either of bad experiences or, more commonly, the sustained effort concentrated on phishing training and awareness [9]). Yet, in our opinion, this ability comes too late, when the URL is already loaded in the smartphone browser (without any indication by the browser itself that it could be a potentially dangerous URL).

B. Actionable Countermeasures

Despite the absence of proactive phishing QR code detection, we believe that there is a room for providing user-centered protection by addressing the design of the QR code scanner apps. Usable security has been of a great benefit to people against phishing, cuing them on insecure websites, lack of certificates, or suspicious emails, and we believe that this approach merits consideration. In particular, we support the idea of providing just-in-time (i.e., appearing as the element is interacted with) and just-in-place (i.e., appearing next to the interacted element) trustworthy URL tips to help people judge links embedded in QR codes, suggested in [36] as an effective way for cuing people on dangerous URLs in emails.

One such usable security solution recommends presenting the actual URL with the domain name highlighted, a tooltip with border color-coded on the level of phishing risk, a brief trustworthy URL tip about the possible dangers of opening it in a browser, and delayed link activation for a short period to give users some time to inspect it before they click [59]. These URL trustworthiness tips appear when a user hovers their mouse over an embedded link in an email (just-in-time)

and right next to the link (just-in-place). The trustworthiness URL tooltips were shown to make a significant improvement in phishing detection in emails by 85.17% versus 43.31% without them [59]. Therefore, we reasonably conjecture that similar adaptations to QR code scanner apps would possibly improve QR code phishing detection among users (noting that user studies are needed to produce hard evidence of the cuing utility, which have not been performed yet).

The tooltips are presented to people depending on the deduced risk of a given URL, e.g., URL structure, presence of non-ASCII characters, presence of short URL services, etc. For use in mail clients, the risk that a given URL is phishing or contains malware is classified on three levels, based on the domain name of the URL as well as potential mismatch between the email link hypertext and the URL behind it:

- ***Low risk*** - means that the URL domain name is on the list of trusted domains provided by the mail client and extended by the user
- ***Unknown risk*** - means that the URL domain name is not yet known and must be checked carefully by the user before it is classified as low risk
- ***Unknown with indicators towards high risk*** - means that the URL domain name contains indicators commonly used in phishing attacks, such as prefixing a trusted domain like "paypal.com" with "secure-"

We propose a QR code scanner adaptation of the TORPEDO add-on from [59] – shown in Figure 3, aimed at warning users about the potential risk of becoming a phishing victim through the QR codes they just scanned. It uses similar techniques to assess risk as the email client variant and it helps people to identify the URL by highlighting the domain, while also explaining how the risk level was determined and what it means in this case. For example, if a shortening service is used, as it was in our *implicit-phishing URL* variant, the enhanced QR code scanner app with user support would provide a brief URL trustworthiness tooltip, so the user has the opportunity to inspect the link before opening it in their browser.

Additionally, in every risk level except low risk, a timer – similar to the TORPEDO add-on [60], [59] – could also be used for the QR code scanner app to give the individual time to focus on inspecting the domain name of the URL, which was shown to be important for decreasing the potential susceptibility to phishing [36]. This interface "friction" could be sufficiently potent for those 57% of our participants to deem this interaction as "strange" and help them to abandon the suspicious URL altogether. Similarly, a list of trusted domains could be built into the QR code scanner that users would both automatically expand and manually append after they have checked the domain name of a link they scanned from a QR code, resulting in a low risk case the next time.

For example, in our proposed adaptation, the *legitimate URL* https://supportukranianconflict.com/, as well as the *explicit-phishing URL* https://phishmeforukraine.com/, would be an unknown risk at first. While people might recognize the word "phish" in the explicit-phishing domain and not open the link, they have the opportunity to add the legitimate URL to their trust list. While the original email variant uses unknown with indicators towards high-risk level for deciding on which URL trustworthiness tooltips to show to the email user, we would argue that there is no need for such a case with QR codes because modern web browsers already maintain a list of known phishing websites using the Safe-Browsing API[1] and block any request to such URLs.

On the other hand, if we were to implement such a block list, it would mean that the enhanced user support would be dependent on a third party, which in turn, would slow down the process of scanning the QR code and eliminate the inherit convenience of quick website access in the first place. Furthermore, such an implementation could raise additional privacy concerns if the block list is updated over the Internet, as the QR code scanner app will need to periodically connect to the block list server to get the latest update. With each connection, the IP address is passed to the block list server, allowing the approximate location of the user to be tracked over time. Also, an implemented block list is effective only when the malicious URL is already listed, necessitating users to verify URLs themselves regardless to be certain. While there may be good reasons for the web browser to use such a regularly updated block list, we consider it unacceptable for any adaptation that pertains to minimize phishing and any other threats overall associated with QR codes.

C. Implications for current Awareness Measures

As shown in [30], the vast majority of anti-phishing advice is focused on email phishing. Although this is understandable, considering that email is still the main phishing attack vector [56], the lack of knowledge about less prevalent, but rising [18], attack vectors leaves users exposed to phishing threat without much protection. Considering that phishers rapidly take advantage of lack of preparation [57], it is important to expand the current anti-phishing measures to cover relatively novel attack vectors too. Yet, the simple expansion of the current recommendation corpus is most likely not going to help coping with the situation, as it might end up inducing security fatigue in the users, i.e., ignoring some time-intensive security recommendations to reach one's goal [50]. To rectify this, a more cooperative type of interventions were proposed in [63], such as the one described in section V-B above.

Although we acknowledge the merits of the interventions proposed in [63], we still believe that awareness measures should not be disregarded. One way to avoid security fatigue and reduce the number of recommendations is to provide users with transferable knowledge, i.e., recommendations that could be applied in more than one context. For example, information on the URL structure is mostly independent from the attack vector used, therefore it could be presented in a format that allows people to understand how to read a URL and then specify where URLs are shown in different contexts (e.g., tooltip, status bar, QR code scanner app, etc.). Unfortunately, this is not the case [38], even though URL analysis is an important factor of email phishing prevention too.

This is further demonstrated in [35], [1], [63], which found that people have little understanding of the URL structure and domain names. This is clearly problematic in any phishing context, but it is especially so when QR codes are the attacking vectors, as the URL is ultimately the only place where people could look for clues. The lack of transferable knowledge can be

[1]Google Safe-Browsing - https://developers.google.com/safe-browsing

(a) Default QR code scanner when scanning a shortened URL

(b) With user support when scanning a shortened URL

(c) With user support when scanning an URL of a trusted page

Fig. 3: Phishing Tooltips within a QR Code Scanner App for Enhanced User Support

noticed also in the reliance of our participants on checking the landing web page layout and content for legitimacy. Distrusting web pages should be a notion already covered in the current anti-phishing material, as it is also relevant for emails, but this does not seem to be the case. The same can be said regarding opening the link. In other words, it might be that the current anti-phishing material is not only lacking QR code specific recommendations, but it is also failing to describe adequately (i.e., in a transferable way) the knowledge it presents.

Another important aspect is the lack of coverage regarding potential privacy threats, such as information shared between apps and trackers. It should be explained that meta-data on the use of mobile phones could be potentially impactful on the privacy of the users [16]. Although privacy risks of desktop and laptop computers is relatively known to users, it is important to convey to people that scanning a QR code and visiting a website, even a legitimate one, might expose them to the analysis of their data traffic, marketing profiling and other privacy intrusive practices. Albeit these are not necessarily tied to phishing, these privacy intrusive practices can still be weaponized by malicious actors, for example to analyze the traffic and determine which susceptibility factors might work the best for a given QR code phishing attack (as seen by 52% of our participants being attracted by the topic itself). Our results, thus, provide further evidence on the need for a general re-evaluation of the current anti-phishing measures, with a focus on transferable knowledge to both reduce the potential for security fatigue and to offer the general population a more holistic approach to protect their security and privacy.

D. Broader Impacts of our Study

In the previous sections of the discussion we covered our results from different angles, but here we want to add general messages that the usable security community should consider actionable, based on the findings from our study:

- An evidence that a phishing threat associated with QR codes has intrinsic features that warrant a more broad attention to aspects normally not considered, such as the pretext topic, format, and design used in the attack vector;
- A need for actionable countermeasure redesign of QR code scanner apps using similar usable security interventions developed against email phishing
- A call for a thorough evaluation of current anti-phishing measures that considers transferable knowledge, to provide people a holistic understanding of the nature of the phishing threat and reduce the threat of security fatigue.

As next stage of how research, we will both evaluate the proposed countermeasures and implement the adaption we proposed in section V-B to pursue an all-encompassing anti-phishing measures that include QR codes as attack vectors.

E. Limitations

We note several limitations of our study. The naturalistic settings entailed a restriction to a convenience sample in areas of high pedestrian activity over regular times during the day and weekends. Though we framed our study in "naturalistic settings" – the circumstances where a person unassumingly encounters a QR code and independently chooses to scan and access the embedded URL – we acknowledge that these settings might be too general. For example, we used high pedestrian locations which differ from locations with low pedestrian activity, or locations where individuals actively look for QR codes (e.g., accessing a restaurant menu or paying for parking). This limitation on the generalization is further confirmed by the fact that we worked with a small sample, limited to funding, time, and the considerable resources needed to run a study in settings outside of a laboratory.

We acknowledge that the replication of our study outside the US might not reveal the same rate of exposure to a phishing threat through QR codes. A theme for a pretext different than a humanitarian that incorporates other principles of persuasion

and used other formatting (e.g., a sticker) also limits the generalization of our results. Here, we acknowledge the merits of testing various pretexts and designs and encourage other usable security researchers to do so. Such tests in naturalistic settings, however, are prohibitively difficult in time, money, personnel, and approvals that need to be invested to collect meaningful data, to which we can attest to. And even if various pretexts are compared, this comparison will almost certainly be done with different participant sets, which in turn, would threaten the validity and the reliability of the results. Relative to participant sets, the participants in our study were 18 years or older and our findings might not entirely generalize for age groups below 18 years, given the possibility of different exposures to QR codes or smartphone use patterns.

To avoid exposing our participants to greater than minimal risk in the naturalistic settings of our study, we did not host any malware with automatic installation feature, nor we harvested actual credentials as in realistic phishing campaigns. Therefore, it is possible that many people in the real world might abandon the URL by abruptly closing their browser app, turning off the phone, or any action that will prevent their actual phishing by either malware or fake login websites. While we also determined the event of URL inspection to be driven towards searching for phishing cues and ultimately abandoning the URL, our results suggest that this might not always be the case when people scan QR codes in the real world. It could be entirely possible that the nature of URL inspection will change in the future, in part in relation to redesigns such as the one we propose in section V-B, affecting both the nature of the phishing threat associated with QR code and the way phishing QR codes are handled by scanner applications (and even advanced smartphone browsers). It is also worth mentioning that the nature of the URLs was subjectively determined by us as researchers to be either legitimate, explicitly, or implicitly phishing, which could be of little to no meaning to those participants that didn't inspected the URLs at all.

We used simple QR codes in our study, however, QR codes that include colors, text, and other graphical factors could also decisive in scanning a poster with a QR code. We acknowledge that all of these factors could affect how a user approaches a QR code and inspects the embedded URL for phishing. Finally, another limitation comes from the nature of self-reporting on the participants' behavior regarding opening the URL before or after they inspected it in the QR code scanning app. While some of the participants noted they found the "phish" or the shortened URL as cues potent enough to avoid the URL, we did not look at or have direct access to their phones to ensure that they actually abandoned it or proceeded to open it in their browsers anyhow. In equal degree, it could be possible that those who reported opening the link in their browser might have not actually done so or interrupted this flow, effectively rendering them safe from potentially being phished.

F. Ethical Considerations

Every public study related to phishing threats runs the risk of informing the attackers about what might be conductive to successful outcomes, especially when it comes to tests in naturalistic settings with a novel attack vector as QR codes. Our study is no exception, but we sincerely believe that the benefits of publishing our results will soon and eventually outweigh the costs of potentially falling for phish because our ultimate aim is to raise awareness and help people avoid QR code phishing victimization in general. Here, we would again stress that we checked with each individual participant whether the unwitting (at first) participation in our study caused any harms. None of the participants expressed they experienced anything harmful and were very open to learn more about the threat of phishing through QR codes and in general. We dedicated sufficient time to convey the details of our study, our goals, and provide resources they could use to raise their awareness about phishing in real life [15] (participants were also encouraged to contact us at any point in future if they encounter anything suspicious so we can provide advice and help for them to avoid being phished).

We were careful not to impersonate a real humanitarian aid effort as it was in the real-world phishing campaigns running in the time we conducted our study [48], [33], [29]. This, in our view, would have caused harm to these efforts and ultimately undermined the trust people have in them to provide humanitarian aid. To ensure that our participants, who expressed interested, would ultimately contribute to the humanitarian aid, we offered them the opportunity to access known organizations such as UNICEF and Amnesty International [53], [2]. Each participant took upon our offer, but for privacy reasons we did not asked nor recorded the way the realized their contribution. Here, we encouraged them to share these humanitarian efforts with as many people as possible. We as researchers also privately contributed to each of these organizations. We acknowledge that participants, regardless of our efforts, might have complained about the sensitivity of the topic chosen though none of them did. Therefore, we provided extensive debriefing to each participant to outline the trade off between the risks of doing a naturalistic settings study that is as realistic as possible and the benefits of increasing awareness of the dangers of phishing URLs associated with QR codes, especially during a period where the current QR code scanner apps offer no user support and phishing warnings.

VI. Conclusion

The possibility of a phishing threat through QR codes, so far, has been evaluated in controlled laboratory settings. However, this approach does not account for realistic scenarios that use real-world phishing pretexts. To address this gap, we devised a field experiment to observe people around places where they usually encounter QR codes. We found that many of our participants were unaware that one could insert a potentially phishing link in a QR code and observed that the salient and locally relevant pretext we used was sufficient to expose them to a phishing threat. Some of our participants inspected the URL embedded in the QR code, both before and after it was opened in their browser, but the lack of QR phishing awareness have made it difficult to avoid being phished. In response to this, we proposed a usable security framework aimed to minimize the risk of QR code phishing.

Acknowledgment

This work was supported by funding from the project "Engineering Secure Systems" of the Helmholtz Association (HGF) [topic 46.23.01 Methods for Engineering Secure Systems] and by KASTEL Security Research Lab.

REFERENCES

[1] S. Albakry, M. K. Wolters, and K. Vaniea, "What is this url's destination? empirical evaluation of users' url reading," in *Conference on Human Factors in Computing Systems*, ser. CHI '20. New York, NY, US: ACM, 2020, p. 1–12.

[2] Amnesty International, "Ukraine crisis: Help protect civilians," 2022, https://donate.amnestyusa.org/page/122555/donate/1?ea.tracking.id=W23XXADEVR0P&en_og_source=W23XXADEVR0P&supporter.appealCode=W23XXADEVR0P&gad_source=1&gclid=CjwKCAiA0syqBhBxEiwAeNx9NxTVyadhgV4YqhHz4T6r0SjBGPo-q50sa0XccRimHbjfqdHD69qvGhoChAkQAvD_BwE&gclsrc=aw.ds.

[3] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report," APWG, Tech. Rep., 2023. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf

[4] L. Barr, "FBI warns criminals are using fake QR codes to scam users," 2022, accessed: 2023.05.09. [Online]. Available: https://abcnews.go.com/Politics/fbi-warns-criminals-fake-qr-codes-scam-users/story?id=82371866

[5] M. Blythe, H. Petrie, and J. A. Clark, "F for fake: Four studies on how we fall for phish," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '11. New York, NY, US: Association for Computing Machinery, 2011, p. 3469–3478. [Online]. Available: https://doi.org/10.1145/1978942.1979459

[6] C. Bravo-Lillo, S. Komanduri, L. F. Cranor, R. W. Reeder, M. Sleeper, J. Downs, and S. Schechter, "Your attention please: Designing security-decision uis to make genuine risks harder to ignore," in *9th Symposium on Usable Privacy and Security*, ser. SOUPS '13. New York, NY, US: ACM, 2013.

[7] P. Burda, L. Allodi, and N. Zannone, "Dissecting social engineering attacks through the lenses of cognition," in *European Symposium on Security and Privacy Workshops*, ser. EuroS&PW '21. New York, NY, US: IEEE, 2021, pp. 149–160.

[8] C. Canfield, A. Davis, B. Fischhoff, A. Forget, S. Pearman, and J. Thomas, "Replication: Challenges in using data logs to validate phishing detection ability metrics," in *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Santa Clara, CA: USENIX Association, Jul. 2017, pp. 271–284. [Online]. Available: https://www.usenix.org/conference/soups2017/technical-sessions/presentation/canfield

[9] G. Canova, M. Volkamer, C. Bergmann, and B. Reinheimer, "Nophish app evaluation: lab and retention study," in *Workshop on Usable Security*, ser. USEC '15. Reston, VA, US: Internet Society, 2015.

[10] R. Chouinard, "New quishing campaign shows how threat actors innovate to bypass security," 2021, accessed: 2023.05.09. [Online]. Available: https://abnormalsecurity.com/blog/qr-code-campaign-bypass-security

[11] R. Chugh, "Can your mobile phone get a virus? yes – and you'll have to look carefully to see the signs," 2022, accessed: 2023.05.09. [Online]. Available: https://theconversation.com/can-your-mobile-phone-get-a-virus-yes-and-youll-have-to-look-carefully-to-see-the-signs-181720

[12] R. B. Cialdini, *Influence: the psychology of persuasion; Rev. ed.* New York, NY: Collins, 2007. [Online]. Available: http://cds.cern.ch/record/2010777

[13] J. Cohen, "A coefficient of agreement for nominal scales," *Educational and Psychological Measurement*, vol. 20, no. 1, pp. 37–46, 1960.

[14] CounterPoint, "US Smartphone Market Share," CounterPoint, Tech. Rep., 2023. [Online]. Available: https://www.counterpointresearch.com/us-smartphone-shipments-decline-in-q1-2023-amid-high-inflation-inventory-correction-apple-share-up/

[15] Cyberesecurity and Infrastrucure Security Agency (CISA), "Avoiding social engineering and phishing attacks," 2021, https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks.

[16] W. Dai, M. Qiu, L. Qiu, L. Chen, and A. Wu, "Who moved my data? privacy protection in smartphones," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 20–25, 2017.

[17] European Union Agency for Cybersecurity (ENISA). (2023) Ransomware. ENISA. [Online]. Available: https://www.enisa.europa.eu/topics/incident-response/glossary/phishing-spear-phishing?v2=1

[18] Federal Bureau of Investigation (FBI), "Cybercriminals tampering with QR codes to steal victim funds," Federal Bureau of Investigation, Tech. Rep., 2022, accessed: 2023.05.09. [Online]. Available: https://www.ic3.gov/Media/Y2022/PSA220118

[19] A. Ferreira, L. Coventry, and G. Lenzini, "Principles of persuasion in social engineering and their use in phishing," in *Human Aspects of Information Security, Privacy, and Trust*, ser. HAS 2015. Cham: Springer, 2015, pp. 36–47.

[20] A. Franz, V. Zimmermann, G. Albrecht, K. Hartwig, C. Reuter, A. Benlian, and J. Vogt, "SoK: Still plenty of phish in the sea — a taxonomy of User-Oriented phishing interventions and avenues for future research," in *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*. USENIX Association, Aug. 2021, pp. 339–358. [Online]. Available: https://www.usenix.org/conference/soups2021/presentation/franz

[21] K. Gibson, "Want to help people in Ukraine? Here are ways to donate," 2023, accessed: 2023.05.09. [Online]. Available: https://www.cbsnews.com/news/russia-ukraine-refugees-donations-charity/

[22] I. Gosting. (2021) How the pandemic saved the qr code from extinction. https://www.forbes.com/sites/forbescommunicationscouncil/2021/03/25/how-the-pandemic-saved-the-qr-code-from-extinction/.

[23] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM*, vol. 50, no. 10, pp. 94–100, 2007.

[24] T.-W. Kan, C.-H. Teng, and M. Y. Chen, "QR Code Based Augmented Reality Applications," in *Handbook of Augmented Reality*. New York, NY, US: Springer, 2011, pp. 339–354.

[25] L. Kersten, P. Burda, L. Allodi, and N. Zannone, "Investigating the effect of phishing believability on phishing reporting," in *European Symposium on Security and Privacy Workshops*, ser. EuroS&PW '22. New York, NY, US: IEEE, 2022, pp. 117–128.

[26] K. Krombholz, P. Frühwirt, P. Kieseberg, I. Kapsalis, M. Huber, and E. Weippl, "QR code security: A survey of attacks and challenges for usable security," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*, ser. HAS 2014. Cham: Springer, 2014, pp. 79–90.

[27] T. Lin, D. E. Capecci, D. M. Ellis, H. A. Rocha, S. Dommaraju, D. S. Oliveira, and N. C. Ebner, "Susceptibility to spear-phishing emails: Effects of internet user demographics and email content," *ACM Trans. Comput.-Hum. Interact.*, vol. 26, no. 5, Jul. 2019. [Online]. Available: https://doi.org/10.1145/3336141

[28] V. Mavroeidis and M. Nicho, "Quick response code secure: A cryptographically secure anti-phishing tool for QR code attacks," in *Computer Network Security*, ser. MMM-ACNS 2017. Cham: Springer, 2017, pp. 313–324.

[29] S. McCallum, "Deplorable scam emails fake fundraising for ukraine," 2022, https://www.bbc.com/news/technology-60836962.

[30] M. Mossano, K. Vaniea, L. Aldag, R. Düzgün, P. Mayer, and M. Volkamer, "Analysis of Publicly Available Anti-Phishing Webpages: Contradicting Information, Lack of Concrete Advice and Very Narrow Attack Vector," in *European Symposium on Security and Privacy Workshops*, ser. EuroUSEC 2020. New York, NY, US: IEEE, 2020, pp. 130–139.

[31] S. Murphy, "Laravel QR code generator infected with malware," 2021, accessed: 2023.05.09. [Online]. Available: https://www.kernelmode.blog/laravel-qr-code-generator-infected-with-malware/

[32] National Institute of Standard and Technology (NIST). (2023) Phishing - glossary — csrc. NIST. [Online]. Available: https://csrc.nist.gov/glossary/term/privacy

[33] Office of Cybersecurity, "Beware of ukraine-themed phishing scams," 2022, https://it.wisc.edu/scams/beware-of-ukraine-themed-phishing-scams/.

[34] K. Parsons, M. Butavicius, P. Delfabbro, and M. Lillie, "Predicting susceptibility to social influence in phishing emails," *International Journal of Human-Computer Studies*, vol. 128, pp. 17–26, 2019.

[35] E. Pearson, C. L. Bethel, A. F. Jarosz, and M. E. Berman, ""to click or not to click is the question": Fraudulent url identification accuracy in a community sample," in *International Conference on Systems, Man, and Cybernetics*, ser. SMC '17. New York, NY, US: IEEE, 2017, pp. 659–664.

[36] J. Petelka, Y. Zou, and F. Schaub, "Put your warning where your link is: Improving and evaluating email phishing warnings," in *Conference*

on Human Factors in Computing Systems, ser. CHI '19. New York, NY, US: ACM, 2019, p. 1–15.

[37] J. Poushter, M. Fagan, S. Gubbala, and J. Lippert, "Americans hold positive feelings toward nato and ukraine, see russia as an enemy," 2023, https://www.pewresearch.org/global/2023/05/10/americans-hold-positive-feelings-toward-nato-and-ukraine-see-russia-as-an-enemy/.

[38] E. M. Redmiles, N. Warford, A. Jayanti, A. Koneru, S. Kross, M. Morales, R. Stevens, and M. L. Mazurek, "A comprehensive quality evaluation of security and privacy advice on the web," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 89–108. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/redmiles

[39] B. Reinheimer, L. Aldag, P. Mayer, M. Mossano, R. Duezguen, B. Lofthouse, T. von Landesberger, and M. Volkamer, "An investigation of phishing awareness and education over time: When and how to best remind users," in *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, Aug. 2020, pp. 259–284. [Online]. Available: https://www.usenix.org/conference/soups2020/presentation/reinheimer

[40] K. Rekouche, "Early Phishing," *arXiv*, vol. [cs], no. 1106.4692, 2011. [Online]. Available: http://arxiv.org/abs/1106.4692

[41] J. Reynolds, D. Kumar, Z. Ma, R. Subramanian, M. Wu, M. Shelton, J. Mason, E. Stark, and M. Bailey, "Measuring identity confusion with uniform resource locators," in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, ser. CHI '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1–12. [Online]. Available: https://doi.org/10.1145/3313831.3376298

[42] S. Robinson, J. Pearson, and M. Jones, "Q-arrgh! commandeering everyday digital codes," in *Conference on Human-Computer Interaction with Mobile Devices and Services*, ser. MobileHCI '15. New York, NY, US: ACM, 2015, pp. 182–186.

[43] J. Saldaña, *The coding manual for qualitative researchers*. Los Angeles, CA, US: SAGE, 2013.

[44] Scanova Blog. (2024) Qr code statistics 2023: Up-to-date numbers on global qr code usage. https://scanova.io/blog/qr-code-statistics/.

[45] F. Sharevski, A. Devine, E. Pieroni, and P. Jachim, "Phishing with Malicious QR Codes," in *European Symposium on Usable Security*, ser. EuroUSEC '22. New York, NY, US: ACM, 2022, pp. 160–171.

[46] F. Sharevski and P. Jachim, "Alexa in phishingland: Empirical assessment of susceptibility to phishing pretexting in voice assistant environments," in *Security and Privacy Workshops*, ser. SPW '21. New York, NY, US: IEEE, 2021, pp. 207–213.

[47] D.-H. Shin, J. Jung, and B.-H. Chang, "The psychology behind qr codes: User experience perspective," *Computers in Human Behavior*, vol. 28, no. 4, pp. 1417–1426, 2012.

[48] C. Shoichet, "Scammers are targeting sponsors who are trying to help ukrainians reach the us," 2022, https://edition.cnn.com/2022/08/03/us/uniting-for-ukraine-phishing-scam-cec/index.html.

[49] T. Sommestad and H. Karlzen, "A meta-analysis of field experiments on phishing susceptibility," in *APWG Symposium on Electronic Crime Research*, ser. eCrime '21. New York, NY, US: IEEE, 2019, pp. 1–14.

[50] B. Stanton, M. F. Theofanos, S. S. Prettyman, and S. Furman, "Security Fatigue," *IT Professional*, vol. 18, no. 5, pp. 26–32, 2016.

[51] M. Steves, K. Greene, and M. Theofanos, "Categorizing human phishing difficulty: a phish scale," *Journal of Cybersecurity*, vol. 6, no. 1, p. tyaa009, 2020.

[52] D. R. Thomas, "A General Inductive Approach for Analyzing Qualitative Evaluation Data," *American Journal of Evaluation*, vol. 27, no. 2, pp. 237–246, 2006.

[53] UNICEF, "Unicef in ukraine," 2022, https://www.unicefusa.org/what-unicef-does/where-unicef-works/europe/ukraine?gad_source=1&gclid=CjwKCAiA0syqBhBxEiwAeNx9N25fr-Em7DZW7AfT30GsVAUYi4H8xG7gNhMXoXAtBXHz58eWhzA11hoCm3wQAvD_BwE.

[54] A. van der Heijden and L. Allodi, "Cognitive triaging of phishing attacks," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 1309–1326. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/van-der-heijden

[55] A. Vance, D. Eargle, J. L. Jenkins, C. B. Kirwan, and B. B. Anderson, "The Fog of Warnings: How Non-essential Notifications Blur with Security Warnings," in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association, Aug. 2019. [Online]. Available: https://www.usenix.org/conference/soups2019/presentation/vance

[56] Verizon, "Data Breach Investigations Report," Verizon, Tech. Rep., 2023. [Online]. Available: https://www.verizon.com/business/resources/Tabb/reports/2023-data-breach-investigations-report-dbir.pdf

[57] R. Verma and A. E. Aassal, "Spears Against Shields: Are Defenders Winning the Phishing War?" in *International Workshop on Security and Privacy Analytics*, ser. IWSPA '19. New York, NY, US: ACM, 2019, pp. 15–24.

[58] 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," in *Financial Cryptography and Data Security*, ser. FC '13. Berlin, Heidelberg, DE: Springer, 2013, pp. 52–69.

[59] M. Volkamer, K. Renaud, B. Reinheimer, and A. Kunz, "User experiences of torpedo: Tooltip-powered phishing email detection," *Computers & Security*, vol. 71, pp. 100–113, 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404817300275

[60] M. Volkamer, K. Renaud, and B. M. Reinheimer, "TORPEDO: TOoltip-poweRed Phishing Email DetectiOn," in *31st IFIP TC 11 International Conference*, ser. SEC '16. Cham: Springer, 2016, p. 161–175.

[61] R. Wash and M. M. Cooper, *Who Provides Phishing Training? Facts, Stories, and People Like Me*. New York, NY, US: Association for Computing Machinery, 2018, p. 1–12. [Online]. Available: https://doi.org/10.1145/3173574.3174066

[62] E. J. Williams and D. Polage, "How persuasive is phishing email? the role of authentic design, influence and current events in email judgements," *Behaviour & Information Technology*, vol. 38, no. 2, pp. 184–197, 2019.

[63] S. Zheng and I. Becker, "Presenting suspicious details in user-facing e-mail headers does not improve phishing detection," in *18th Symposium on Usable Privacy and Security*, ser. SOUPS '22. Berkeley, CA, US: USENIX, 2022. [Online]. Available: https://www.usenix.org/conference/soups2022/presentation/zheng

APPENDIX

Verbal Script

Dear Madam/Sir,

My name is [redacted], I am a researcher from [redacted] University. My contact number is [redacted] and my email is [redacted]. I am conducting a research study about the decision people to visit a website when interacting with QR codes and I noticed you just scanned a QR code in the nearby poster placed at [PLACE].

The purpose of the research is to learn more about how people interact with QR codes in general. I am recruiting only volunteers for this research study and you can participate on your own volition. You are eligible to participate if you are 18 years or above old, you are from United States, you are able to understand and converse in English language, you holds a internet capable smartphone and you have used a QR code to access a website at least once (which you just did).

I will ask you several open-ended questions and collect some personal information about you. The interview is anonymous and you are asked to participate on a voluntarily basis. If there is a question you do not want to answer, you may ask us to skip it. Your information will be kept confidential and stored in a secured computer under password protection and with encrypted files. The data will be kept de-identified. The participation will take between 5-10 minutes.

I have obtained an IRB protocol [redacted] approval and version date of the document. If you like to contact anyone from our institution regarding this research you may contact [redacted].

Data Collection Distribution

Each poster was placed for the duration of the week (Monday to Sunday) between 10:00AM and 6:00PM at each location. We covered two locations per week due to the restriction in research personnel.

Week	Locations		
	Mall	Cafe	Cultural point of interest
Week 1	4	2	0
Week 2	6	4	0
Week 3	5	0	2
Week 4	3	0	6
Week 5	0	4	2
Week 6	0	3	1
Total = 42	18	13	11

Interview Questions

1) What attracted you to scan this particular QR code? Please explain in your own words.
2) Once you scanned it, what were the next steps you took?
   a) **Clicked on the website**: Did you pay attention on any particular website elements?
   b) **Abandon it**: What were the reasons you decided not to proceed and visit the associated website?
3) Do you usually scan QR codes?
   a) **Yes**: For what services are these QR codes and what steps you do usually take?
   b) **No**: Why not?
4) **Inspection.** When you scan a QR code, do you inspect the domain URL in the displayed frame of the scanner (e.g. do you read the domain displayed on the linked website in the scanning app [yellow bar])?
   a) **Yes**: Do you also inspect the URL further when you open it in the browser?
   b) **No**: Do you perhaps inspect the URL when you open it in the browser?
5) Have you noticed any problems related to the QR codes or the websites they lead to?
6) Do you usually use the default phone app/browser for QR codes or you use other apps/browsers?
7) Demographics: Age, gender, race/ethnicity, education, computer proficiency

Codebook

- **Delivery Vector.** Codes related to the vector used to deliver the phishing attack. The category is divided into two sub-categories.
  - **QR code Vector.** The sub-category collects codes pertaining to the context in which the QR code is presented and the QR code itself.
    - **Topic.** What attracted the user was the topic discussed in the QR code context.
    - **Color.** The coloration of the QR code context was attractive for the user.
    - **Text.** The text of the QR code context was attractive for the user.
  - **General look - Context.** The general look of the vector used is what the user checked.
  - **Poster Size.** The size of the vector used attracted the user.
  - **URL shown.** Codes that describe the URL contained in the QR code and the behavior related to it.
    - **Inefficient Interface.** This category describes users' comments regarding inefficiencies of the QR code scanner used.
    - **URL - App.** Codes describing the inspection or not of URLs in the web address bar.
      - **Tiny URL - App.** The user noticed the use of a shortening service.
      - **Concerning - App.** The user found the URL showed in the App concerning.
      - **Reassuring Terminology - App.** The user noticed the use of words in the URL than led them to judge it as trustworthy.
      - **Not open if suspicious.** The user was suspicious of the URL and decided to not open it because of that.
    - **URL not inspected - App.** Codes describing users that do not inspect the URL of a website reached after using a QR code.
  - **Location.** The location of the delivery vector influence the scan of the QR code.

        - **Restaurant.** The user mainly uses QR codes at restaurants.
        - **School.** The user mainly uses QR codes at school.
        - **Work.** The user mainly uses QR codes at work.
        - **Groceries.** The user mainly uses QR codes while shopping for groceries.
    - **Other.** Umbrella code for information unrelated to the vector itself, but somewhat connected to the single participants looking at it, e.g., the coloration reminded them of something they like.
- **website Vector.** Codes related to the website integrated in the QR code and the behavior of the users on it.
    - **Sensitive data request.** Codes describing specific sensitive information related features of a webpage and their behavior on it.
        - **Email.** The user check if the website requests their email
        - **Sign-up.** The user check if the website requires them to sign-up for the service
        - **Enter info on request.** The user enter any information required to proceed.
    - **website technical features.** This category describes codes related to technical aspects of the website, such as security indicators and URLs, and how users interact with them.
        - **SSL.** The user checks the SSL certificate of the page to determine its legitimacy.
        - **URL - Browser.** Codes describing the inspection or not of URLs in the web browser.
            * **URL inspected - Browser.** Codes describing the interaction of users once the URL is inspected and how often they do so
            * **Concerning - Browser.** The user found the URL used in the study concerning
            * **Different than expected.** The URL used were different than expected or different than in the QR code scanner.
            * **Reassuring terminology - Browser.** The user noticed the use of words in the URL than led them to judge it as trustworthy.
            * **Sometimes inspected - Browser.** The user inspects URLs on websites after using a QR code inconsistently.
        - **Not inspected - Browser.** Codes describing users that do not inspect the URL of a website reached after using a QR code.
        - **Only on desktop/laptop.** The user does not check URLs on mobile devices.
    - **website content.** Codes related to the website content and the users' interactions with it.
        - **General look - website.** The users inspect the general look of the website to determine its legitimacy.
        - **Search for information.** The users read the information presented on the web page to determine their legitimacy.
    - **Other.** Codes related to the website interaction but not tied to anyone category in particular.
        - **No attention paid.** Users did not paid attention to the website.
        - **Self-interest.** The main interest of the user is motivated by self-gain.
        - **Nothing noticed.** The user did not notice anything on the website.
- **Behavior.** This category contains codes describing the general behavior of the users during their interactions with QR codes, the QR code vectors and the websites associated with them.
    - **Link opened.** The user clicked, i.e. tapped or used a voice assistant to instruct the QR code scanner application to open and access the website link.
    - **Link not opened.** The user interrupted their interaction with the QR code.
    - **Unknown action on link .** The user did not disclose sufficient information to infer the outcome of their interaction with the QR code.
    - **Curiosity.** The main driving force of any interaction is curiosity towards the QR code and the associated website.
    - **QR code general use.** Codes describing the general stance towards QR codes.
        - **Only if interested.** The user uses QR codes only if the topic is of interest.
        - **Only if needed.** The user uses QR codes only if required.
        - **Not usually used.** The user usually avoids using QR codes.
        - **Distrust QR codes.** The user distrusts QR codes as a whole.
    - **Strange previous interactions.** Codes describing if users ever experience strange interactions in the past.
        - **No.** The user never experienced strange interactions.
        - **Not often.** The user did experience strange interactions, but only occasionally.
        - **Did not checked.** The user never checked enough to be sure strange interactions occurred.
        - **Depends on attention.** The user noticed strange interactions but admits that this hap-pens depending on their attention level.
        - **Yes.** The user did experience strange interaction. This is then further determined as either related to the URL or Unspecified.

Gender Declared	38% Female			62% Male		
Age Distribution	24% [18-24]	29% [25-34]	24% [35-44]	17% [45-54]	4% [55-64]	2% [65+]

QR code Proficiency	5% Low	42% Intermediate	52% High
Device	6% Not disclosed	12% Samsung Galaxy	82% iPhone
Everyone used their OS default QR Scanner app			