Phishing with Malicious QR Codes

FILIPO SHAREVSKI, DePaul University, United States

AMY DEVINE, DePaul University, United States

EMMA PIERONI, DePaul University, United States

PETER JACHIM, DePaul University, United States

The use of QR codes for malicious purposes was rather limited in the pre-COVID-19 world. That changed overnight, as the QR codes became a convenient go-between for sharing URLs, including malicious ones. This opens an attractive new way of phishing as QR codes are now widespread. To explore phishing with QR codes (i.e. *quishing*), we conducted a 173-participant study where we used a COVID-19 digital passport sign-up trial with a malicious QR code as a pretext. We found that 67 % of the participants were keen to sign-up with their Google or Facebook credentials, 18.5% to create a new account, and only 14.5% to skip on the sign-up. Convenience was the single most cited factor for the willingness to yield participants' credentials. Reluctance of using new services was the reason for creating a new account or skipping the registration. We also developed a *Quishing Awareness Scale* (QAS) and found a significant relationship between participants' QR code behavior and their sign-up choices: the ones choosing to sign-up with Facebook scored the lowest while the one choosing to skip the highest on average. We used our results to propose awareness training guidelines as well as develop and test usable security indicators for warning users about the threat of phishing with malicious QR codes.

CCS Concepts: • **Security and privacy → Social aspects of security and privacy**; **Usability in security and privacy**.

Additional Key Words and Phrases: phishing, QR codes, usable security, phishing awareness training

1 INTRODUCTION

Disruptive in every aspect, the COVID-19 pandemic forced a practical reorganization of our rather comfortable lifestyles. The ergonomic aspect in particular took the hardest hit, outside the devastating public health toll: Mask and distance mandates, virtual work environments, contact-free exchange of goods, and touch-free information transfer [17]. Adopting alternative designs for otherwise intuitive everyday interactions was inevitable to prevent the COVID-19 virus from rapidly spreading [14]. Instead of paper, people got to scan a Quick Response (QR) code with our smartphones to read a restaurant menu or enter a venue, for example. QR codes, initially developed for high-speed tag scanning, are not an entirely new design per se, but were far from being widespread before the requirement for touch-free interaction [37].

QR codes embed a simple piece of information, either a (i) unique identifier that enables external scanning and verification against a back-end database (e.g. barcodes) or (ii) Universal Resource Locators (URLs) that, once decoded through users' smartphone camera, enable direct access to websites (e.g. restaurant menus) without the need to type the link themselves [48]. The simplicity of the information piece itself made the QR codes the prefect candidate for

manipulation. But beside impersonation or duplication, malicious actors were yet to entertain the full potential of manipulating the QR codes to their advantage [43]. However, the more applications adopted QR codes, the more creative attacks exploiting a wide range of victims surfaced [38].

This is especially true for phishers [40]. Controlling malicious URLs (e.g. links to impersonated login websites), phishers are equally keen to adopt new alternative "designs" in luring victims to yield their credentials or download malware [39]. Phishers started simple by luring victims to malicious URLs through unsuspected QR codes [30, 47]. They moved next to embed a malicious URL in a QR code that was itself embedded in another QR code knowing that the inner one is scanned first before the outer, legitimate one [22]. Phishers even became prolific in sophisticated alteration of the codes pixels of unsuspected QR codes to embed the malicious URL without the need for physical tampering [78].

The practice of "*quishing*" or phishing with malicious QR codes (i.e. QR codes that embed a malicious URL) is not new, but so far affected a small number of victims and thus never received much of an attention [19]. QR codes' lack of widespread adoption certainly was the main limiting factor in the pre-COVID-19 world. But quishing popularized when QR codes became the essential go-between for information sharing [54]. For example, malicious QR codes were found on parking meters throughout San Antonio, directing victims to a fraudulent website to submit payment to a fraudulent vendor [6]. Quishers attached same-day generated malicious QR codes to emails to evade URL detection (unlikely to be updated to block QR code images) in a phishing campaign attempting to collect Microsoft credentials [19]. And quishers elegantly included a backdoor in an open-source QR code generator that contains malware which they could use to remotely execute code on a compromised machine or install and access a remote shell [51].

The proliferation of quishing certainly warrants a response, not just by issuing user advisories [54], but also exploring pretexts and tactics, gauging users' susceptibility, and raising users' awareness. To these objectives, we "went quishing" in a field study with 173 participants. The pretext we created was a sign-up for a COVID-19 digital passport trial aiming to replace the paper vaccination cards issued by the Centers of Disease Control (CDC) [16]. We incorporated a malicious QR code within a legitimate-looking CDC poster borrowed from their Toolkit for General Public communication [18]. We observed the sign-up choice for each participant (Facebook or Google credentials, creating a new account, or skipping a sign-up) and collected information about participants' practice of using QR codes.

Our observations show that 67 % of the participants opted to use either their Facebook or Google credentials, 18.5% to create a new account, and only 14.5% to skip on the sign-up. Using our results, we developed a *Quishing Awareness Scale* (QAS) following the approach for measuring proactive phishing awareness in [25]. We found a significant relationship between participants' QAS score and their sign-up choices: the participants who opted for the Facebook route scored the lowest and the participants who opted to skip the sign-up scored the highest on the QAS scale. Using these results we created actionable quishing awareness training guidelines incorporating the wealth of previous phishing awareness knowledge and practice [31, 73]. We also utilized various usable security recommendations to develop and test practical anti-quishing security indicators in a follow-up study [26, 57, 74].

Following this introduction, we outline the past and present approach of quishing in Section 2. We then elaborate on our pretext, quishing tactics, and measurements in Section 3. Section 4 provides the results of our study. Section 5 outlines our anti-phishing training guidelines and the usability tests we conducted to evaluate quishing indicators we proposed. The overall findings are discussed in Section 6 and Section 7 wraps the paper.

2   BACKGROUND RESEARCH

2.1   How Users Fall for Phish

Phishing, in the most common example, involves an attacker sending an email asking the user to click on a URL and enter in their credentials on the resulting website [73]. The resulting website does mimic the appearance of a website from a trusted organization (e.g. a bank or Gmail), but it does so on the surface. In the background, the resulting website is associated with a malicious URL and is controlled by the attacker. The user has no way of knowing, unless carefully inspecting the URL and the website's layout [52], that the entered credentials end up in the attackers hands instead [61].

Phishing works time and again for several reasons. The "asking" part in the email incorporates a persuasive pretext sufficiently potent to incite an action by the user. The attacker knows well that there are fundamental vulnerabilities of human cognition - or 'shortcuts' - that determine decisions on the basis of previous experiences, biases, or beliefs [20]. So when the email is "signed" and comes from a bank or Gmail, the user feels compelled to comply with these *authorities* [65]. Even more, if the email says that the user must "update the account within 24 hours or loose access," then the user feels the *urgency* to do so [44]. Sometimes, the asking comes with a small reward ("sign-up with your Gmail account, get an Amazon gift card") making the user feel obliged to *reciprocate* [8]. Sometimes, users are provided a *social proof* that other users, some of whom they *like* or share similarities with, already took the action asked [28].

Despite being persuaded to click on the link, users still have an option to avoid being phished. The resulting websites sometimes present typographical errors and visual discrepancies related to the typeface, design layout, or logos [50]. So users, if paying attention, could spot misspellings, grammatical errors, inconsistency between mobile and desktop versions, and perhaps deprecated logos. But that's not always the case and these discrepancies remain unnoticed by most of the phishing victims [3]. Even if the resulting website appearance could be indistinguishably mimicked, attackers must deviate the malicious URL from the legitimate one to redirect the user [69]. Spotting a malicious URL remains a hard problem for humans [64], but modern email clients and browsers are better in detecting the malicious URLs, so they employ preemptive indicators of potential phishing to warn the users [63]. Users, unfortunately, often ignore these indicators because they are confusing, interfere with the primary task of entering credentials, or users are not technically proficient to understand them [27].

2.2   How Users Fall for Quish

In quishing, or phishing with QR codes, the attacker does not have the advantage of using an email. Here the malicious URL has been either embedded in the QR code itself [22, 47] or the QR code layout manipulated to redirect the user to override the URL of the trusted organization [39, 78]. Assuming this is successful, the attacker must adapt the persuasive pretext to fit with the natural usage of QR codes i.e. all "shortcuts" might not work. Looking *authoritative* by adding QR codes in an email supposedly coming from a bank or Gmail did yield some success [19], emails with a QR code could be easily filtered out. The next thing is to try to assume authority of a convenience service like in the case of parking meters [6] or bus stop schedules [47], but one could simply use a smartphone application instead of a QR code.

Assigning *urgency* (*scarcity* in general) for the purpose of scanning a QR code could work given that users that fell for quish so far did it so mostly out of curiosity [71]. In this case, coupling with *reciprocation* could work well too, because it creates a tangible proposition for a user to scan a QR code in the first place, e.g. participate in a study. The *social proof* is naturally helpful in such pretext, provided the QR codes are placed where usual study recruitment takes place - college campuses, for example - because others also participate too. The topic for the study could be something that naturally fits what a user in such a setting might like: self-determination, social networking, or campus life.

Another conducive factor to quishing is that humans do not get much of a help in spotting malicious QR codes. For example, incorporating security primitives in QR codes creates an overburdening computational delay (e.g. users start aborting the scanning) [30, 47]. A trusted organization could create a QR code with distinctive properties, e.g. logos [40], but it is increasingly trivial for attackers to duplicate and impersonate such codes. The smartphone's QR scanning function and browsers could incorporate usable security indicators, but nothing says users would not ignore these too [13]. Quishing advisories, as the one from the Federal Bureau of Investigation (FBI) [54], do attempt to raise awareness but are far from a comprehensive approach comparable to the awareness work done for phishing [31, 64].

3 MALICIOUS QR CODES

What is still largely unknown is how users could fall for quish if the pretext is outside of a college campus setting or places like bus stops with limited number of people. The established trusted norm of using QR codes during COVID-19 provides an ideal opportunity to do such tests since it drastically expanded the number of users as potential participants meeting the "inclusion criteria" for quishing studies. Now almost everyone has used a QR code at least once already and chances are high we will keep doing so in the foreseeable future [14]. So a quishing study in these settings must not just explore the workings of quishing on a larger scale, but produce actionable deliverables of immediate anti-quishing help. To these points, we design a usability study pertaining to answer the following research questions:

RQ1: How users are susceptible to phishing with malicious QR codes, e.g. quishing?
**RQ2**: How one's quishing awareness factors in their susceptibility to quishing?
RQ3: How the results from a quishing field study could be help training for users not to fall for quish?
RQ4: What security indicators could help users spot malicious QR codes?

3.1 Quishing Pretext and Infrastructure

The pretext in our study employed several elements targeting the users' shortcuts regularly exploited in both phishing and quishing so far. To appear *authoritative*, the pretext invited participants to sign up for a COVID-19 digital passport trial aiming to replace the paper vaccination cards issued by the Centers of Disease Control (CDC) [16]. The attention to CDC during the COVID-19 pandemic ensured participants have heard of it and it was successfully used as an authority in phishing already [15]. Unlike other countries' health authorities, CDC has not yet issued a digital vaccination passport despite the convenience of such tool for proof-of-vaccination in businesses or travel [23]. Efforts to do so were signaled by the US health authorities, but nothing yet has materialized up and during our study window, so it was fairly reasonable for participants to believe a trial for vaccination passports would take place (trials during the initial COVID-19 vaccine development received detailed media attention, for example [46]).

Using the CDC's media communication toolkit and [18], we developed a flyer for the COVID-19 vaccination passport trial shown in Figure 1a. We paid attention to mimic the appearance of the regular CDC communication on social media assuming most of the users would have already been exposed to posts with very similar design. The flyer also enabled us to overcome the absence of a traditional email communication and include a verbose persuasive text. We used an authoritative yet optimistic premise for the need of a digital vaccination passport and provided an analogy with the traditional "yellow card" passports [32]. We employed *scarcity* by pointing out the "proof-of-vaccination requirement" as a requirement for entering venues and travel (at the time of the study), as well as implicit *reciprocation* and *social proof* since the "sign-up is quick and easy; use the passport anytime, anywhere." Participants, we assumed, have already
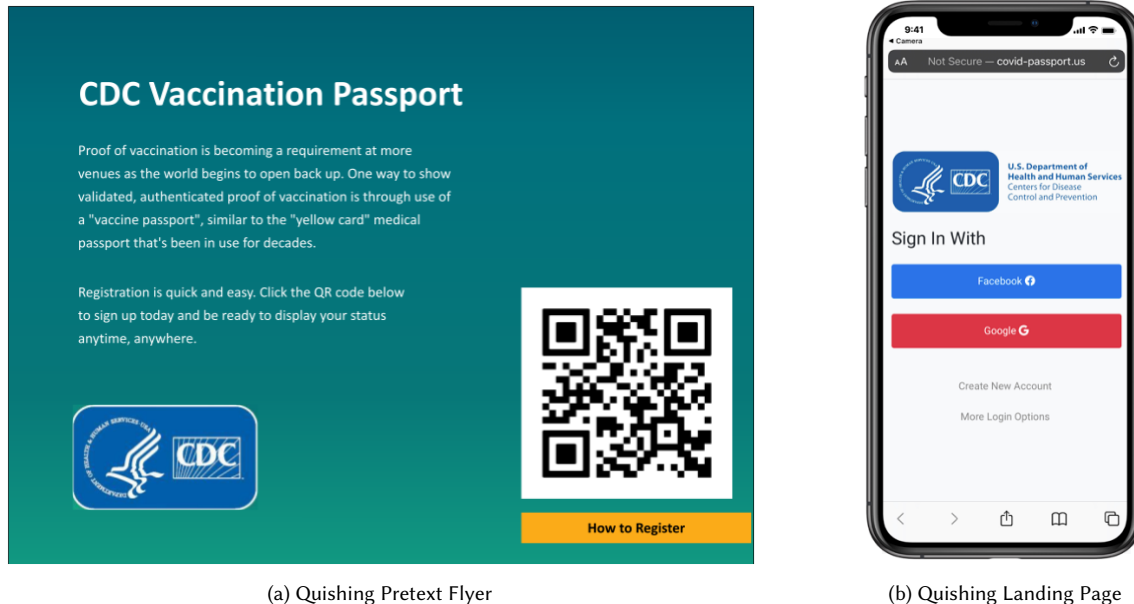
(a) Quishing Pretext Flyer

(b) Quishing Landing Page

Fig. 1. Quishing Infrastructure

felt the analogous social proof with the paper vaccination cards and would reciprocate by joining the trial and scanning the QR code in the flyer for the convenience of having a proof-of-vaccination on their smartphones instead.

The QR code from the flyer directed the users to http://covid-passport.us/qr, a URL we established just for this project. The landing page of the resulting website is shown in Figure 1b. The landing page retains the CDC logo we used in the flier and employs a minimal design centered around the options for sign-up. We ran an experimental pilot study to determine the most popular ways of signing up that confirmed Facebook and Google as the preferred Single Sign On (SSO) providers [7]. We mimicked the SSO buttons to lead users to Facebook and Google login options. We also included the option for the participants to create a new account or to skip using any credentials. To avoid registration, they had to first click on the "More Login Options" link which showed the "Skip" button. We introduced an extra step to observe if the participants would take it to stay secure.

The Institutional Review Board (IRB) approved both a pilot and a main study. However, IRB did not allow us to collect participants' actual credentials. When the participants clicked the SSO and were about to land on Facebook and Google impersonated login options, we redirected them to an individual survey link where they were asked open-ended questions to rationalize the choice of login, elaborate on their individual use of QR codes, and answer quishing awareness-related questions (in a randomized order for each participant). Both reputation and attention checks were included to prevent machine-generated inputs and poor responses. The survey was anonymous and allowed users to skip any question they were uncomfortable answering.

We did obtain a non-full disclosure approval from the IRB which required collecting a consent before the exposure to the quishing poster. Our inclusion criteria stipulated participants to be from the US, 18 years old, and familiar with CDC vaccination cards. Each participant, recruited through Amazon Mechanical Turk, was initially directed to a separate consent page that contained the poster with the QR code for the trial. Each of the branching surveys included

a debriefing statement at the end explaining the deception used in the quishing study. Participants had the option to ask their data to be removed (no one did so). Participants were compensated $18 per hour for a 20 minute study, which we advertised as a "COVID-19 Digital Vaccination Passport Trial."

3.2 Quishing Awareness Scale

The stipulation for no direct collection of participants' credentials helped us avoid situations where the participants would drop the survey feeling being tricked. Retaining participation was useful for us to collect data and measure participants' underlying psychological constructs when interacting with QR codes. Since quishing is a variant of phishing, we looked at adapting existing scales that measure end-user behaviors when dealing with malicious URLs. One such scale is the *Security Behavior Intentions Scale (SeBIS)* [25]. The SeBIS scale consists of 16 items that measure 4 underlying constructs: device securement, password generation, proactive awareness, and updating behaviors. Interacting with QR codes is not directly dependent on any of the these constructs except the "proactive awareness" because one is proactively phishing aware if they take into account security indicators of suspicious URLs and resulting websites (e.g. checking before clicking on links or submitting credentials). The SeBIS proactive awareness sub-scale showed good performance and was used for measuring in numerous phishing experiments [45, 60, 65].

We modified the proactive awareness sub-scale questions to focus particularly on behavior around malicious QR codes and created the *Quishing Awareness Scale* (QAS) as shown in Table 1. The first two QAS questions capture the routine behavior when interacting with QR codes analogous to (not) inspecting URLs and visual websites during everyday browsing. The third and forth QAS questions capture the behavior when faced with security indicators or lack of thereof. Each question is reversely scored and averaged to yield the resultant QAS score. Low scores on the SeBIS score have been related to impulsivity, risk-taking, and dependence (i.e. seeking help from others) [10] and users who did not fail for phish score significantly higher than the rest [25]. As phishing and quishing are heavily related, one could reasonably expect the proposed QAS to capture a similar manifestation when measuring quishing awareness as SeBIS, already a validated measure, measures phishing. We also performed a concurrent validity test between the two scales to establish a formal evidence of QAS's validity as part of our pilot study [24]. Both scales were significantly correlated $r(24) = .937, p = 0.001$ The QAS scale also showed a reliable internal consistency with Crombach's $\alpha = .728$.

Table 1. QAS and SeBIS: Questions (reversely scored and averaged to yield the resultant score)

#	Scale	Questions
1	QAS	When I scan a QR code, I open the link without first verifying where it goes
	SeBIS	When someone sends me a link, I open it without first verifying where it goes
2	QAS	I know what website I'm visiting based on its look and feel, rather than by looking at the QR code or the URL bar.
	SeBIS	I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.
3	QAS	I submit information to QR code websites without verifying it is sent securely (e.g., SSL, "https://", a lock icon).
	SeBIS	I submit information to websites without first verifying that it will be sent securely (e.g., SSL, "https://", a lock icon)
4	QAS	When scanning QR codes, I read the links to see where they go, before clicking them.
	SeBIS	When browsing websites, I mouseover links to see where they go, before clicking them.
5	QAS	If I discover a security problem with the QR code or the website, I continue what I was doing because I assume someone else will fix it.
	SeBIS	If I discover a security problem, I continue what I was doing because I assume someone else will fix it
Scale: Never (1), Rarely (2), Sometimes (3), Often (4), and Always (5).		

3.3 Pilot Quishing

Before we did our main study, we conducted a pilot study with 24 participants to verify the pretext, the quishing workflow and protections, and debug the process before recruiting a larger sample. We also used the pilot study to validate the QAS scale. None of the pilot participants suspected the pretext, the URL, or resulting sign-up website. In the first half of the study, Facebook was the first sign-up option, followed by Google, Twitter, "new account", and "skip." The debriefing uncovered that the "skip" option enabled participants to immediately avoid using anything related to social media for which they expressed a high skepticism.

We therefore decided to experiment by hiding the "skip" option behind an extra click of "More Login Options." This proved a good tactical step from a quisher's point of view since only one user took the pains to click and skip the sign-up. We noticed a lack of interest for the Twitter SSO so we eliminated it in the main study. The pilot study results indicated that Facebook was the most convenient to sign-up with, followed by Google. Participants deemed their Google credentials more "valuable" than Facebook stating that they "*don't mind having their Facebook login shared elsewhere*" even if it gets compromised. The participants that chose Facebook had the lowest average score $\overline{QAS} = 1.56$ and the ones that skipped the sign-up scored the highest on average $\overline{QAS} = 2.58$.

4 MAIN QUISHING STUDY

After the consolidation and consistency checks, we recruited a total of 173 participants. The sample contained 44.2% female and 55.8% male participants. Most of them were college graduates (60.1%), followed by high school graduates (28.3%), post graduates (10.4%) and only 2% participants with less than a high school education. Age-wise, 45.7% were in the [35-44] bracket, 24.3% in [25-34], 13.9% in [45-54], 9.8% in [55-64], and 6.4% in [18-24]. Asked about their QR code usage, 32.4% reported using QR codes "regularly," 56.1% "only when QR codes were preffered" type of information exchange, and 11.6% said "only when QR codes were required."

4.1 Quishing Susceptibility (RQ1)

Out of 173 participants, 44.5% choose Google's SSO for sign-up, 22.5% choose Facebook, 18.5% chose to creating a new account, and only 14.5% choose to skip the registration for the alleged COVID-19 digital vaccination passport trial. The open-ended responses in the survey were coded independently by two researchers on the main decisive factor for their sign-in choice (excellent inter-coder agreement - Cohen's κ = .981). The Pearson's chi-square test revealed a statistically significant relationship between the sign-up choices and justification factors, $\chi(3) = 106.978$, $p = .000^*$, tabulated in Table 2. Convenience was the factor cited by almost 90% of the participants that opted for Facebook, quoting that "*creating an account seemed like a process that might take too long, and I prefer using Facebook to log-in*" [**Participant (P)97**]. Interestingly, the participants citing personal safety quoted: "*I prefer to use Facebook for experimenting with new apps because I don't want spam in my email accounts*" [**P39**]. The only participant suspicious of quishing provided an interesting explanation: "*I wasn't sure if I can trust this link so I'd rather compromise my Facebook login and then change the password later if needed*" [**P17**].

None of the participants that selected Google's SSO was suspicious of quishing, but a good 20% of them preferred using their Google credentials over Facebook citing: "*I don't want to associate this vaccine passport with my Facebook so I chose Google*" [**P50**]. Almost 13% of the participants cited personal safety for their Google choice because they "*believe Google more than Facebook, to keep [their] data safe*" [**P76**]. Anecdotally, one these participants said: "*I trust the use of my Google account as a passport but also found the site to look reliable enough to be trustworthy. Nothing in the URL*

Table 2. Sign-up Choice Justifications

Factor	Facebook	Google	New Account	Skip
Convenience	35	51	3	7
Perceived Safety	3	10	8	12
SSO Reluctance	0	0	13	5
Distrust	0	16	4	0
Suspicious	1	0	4	1
Total	39	77	32	25

seemed out of the ordinary" [**P72**]. The remaining 64% simply preferred Google because it was the "*easiest method of logging in*" [**P156**].

Expectantly, the participants that opted for creating a new account predominantly cited a reluctance to use either Google or Facebook for sign-in to "*link [their] existing accounts with the passport*" [**P109**]. Those who opted for personal safety reasons indicated they have "*privacy concerns*" about the COVID-19 digital vaccination passport [**P162**]. Equal percentage of these participants - 12.45% - distrusted Facebook and were suspicious of the link/website. A couple of the participants did not trust the website, one questioned the website's visual appearance, and one actually used a browser security indicator to suspecting something is "phishy:"

P37: "*I don't know how trustworthy the site is. I would prefer to not use my main email in case it is spam.*"

P79: "*I don't trust that website with my information. It looks like an official us government site but it's not*"

P123: "*I'm not familiar with this platform and did not trust it to link to existing accounts I have. Also, the website was not secure in the browser address bar.*"

P166: "*I don't fully trust the site and didn't want to link my Google account to anything that wasn't 10000% safe*"

The participants that went the extra step to skip registering cited time as a convenience in 28% of the cases, noting that "*...not creating a login saves me time*" [**P163**]. In 48% of the cases participants cited concerns about their privacy: *I did not want any of my personal accounts to be connected with a vaccine passport because a vaccine passport is private medical information* [**P21**]. In 25% of the cases, social media distrust factored the most in skipping the sign-up: "*I am not comfortable linking social media with my vaccine passport*" [**P116**]. Only one participant was suspicious about the COVID-19 digital vaccination passport: "*I didn't want to log in with my Facebook or Google account because I wasn't sure how safe and secure this website is*" [**P113**].

4.2 Quishing Awareness (RQ2)

To understand how a possible awareness of threats from malicious URLs associated with QR codes relates to participants' choices for sign-in, we asked the participants to answer each of the QAS scale items from Table 1. Since not all of the choices formally satisfied the test for normality, we performed a non-parametric Kruskal-Wallis test to compare whether there is a difference in the QAS score between the participants from each of the sign-up groups. Indeed, the result was statistically significant $U = 15.335$ & $p = .002^*$ with the distribution of the scores per group shown in Figure 2. The participants that chose Facebook scored the lowest on the scale on average($\overline{QAS} = 2.41, \sigma = .895$), followed by the ones that selected Google ($\overline{QAS} = 2.64, \sigma = .765$) and new accounts ($\overline{QAS} = 2.69, \sigma.631$). The highest score on average ($\overline{QAS} = 3.18, \sigma.575$) had the participants that chose to skip the sign-up for the COVID-19 digital vaccination passport.
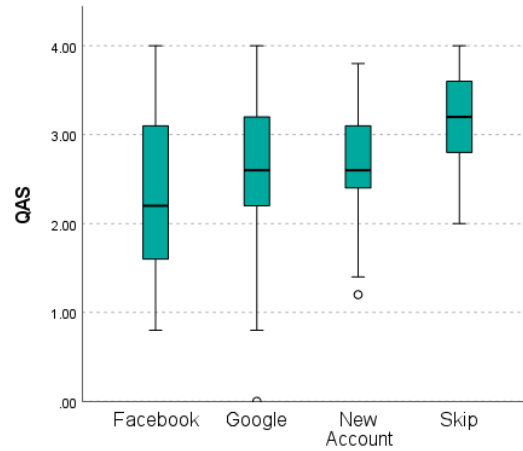
Fig. 2. QAS Score Distribution Per Sign-up Choice

When grouped per justification, the suspicious participants scored the highest ($\overline{QAS} = 3.00, \sigma = .551$), followed by the ones that distrusted Facebook ($\overline{QAS} = 2.81, \sigma = .678$), the ones reluctant to use SSO ($\overline{QAS} = 2.72, \sigma = .539$) and the ones concerned about their online safety ($\overline{QAS} = 2.72, \sigma = .647$). The lowest score had the participants that choose convenience ($\overline{QAS} = 2.60, \sigma = .881$) as a reason. Table 3 shows the average QAS score per each category of justification for each of the sign-in choices. The participant that chose Facebook but cited lack of trust in the website scored the highest on QAS. So did the participants that chose Google but cited personal safety, although the remaining justifications are on comparable levels of quishing awareness. The participants that chose to create a new account because of convenience or personal safety scored the lowest while the the ones expressing distrust in Facebook or suspicion in the resulting website scored the highest. The participants that chose to skip scored consistently high regardless of the justification provided.

Table 3. QAS Average Scores and Standard Deviations

Factor	$\overline{QAS}$	σ	$\overline{QAS}$	σ
	Facebook		**Google**	
Convenience	2.44	.93	2.62	.83
Perceived Safety	2.00	.529	2.72	.518
SSO Reluctance	0	0	0	0
Distrust	0	0	2.72	.696
Suspicious	2.60	/	0	0
	New Account		**Skip**	
Convenience	2.45	1.275	3.29	.62
Perceived Safety	2.4	.534	3.12	.617
SSO Reluctance	2.63	.467	3.16	.572
Distrust	3.25	.678	0	0
Suspicious	3.05	.66	3.20	/

We also performed a Kruskal-Wallis test to compare whether there is a difference in the QAS score between the categories of QR code usage or participants' demographic identities. The QAS score has a statistically significant

difference only between the categories of QR usage as shown in Figure 3, $U = 6.594$ & $p = .037^*$. Participants that used QR codes regularly had the lowest average score ($\overline{QAS} = 2.60, \sigma = 0.779$) but not far away were the participants that opted for using QR codes as a preferred touch-free information transfer ($\overline{QAS} = 2.64, \sigma = 0.762$). The participants that used QR codes only when required scored noticeably higher on average ($\overline{QAS} = 3.08, \sigma = 0.774$). Participants' level of education, gender identity, or age did not significantly factor in participants' quishing awareness scores.
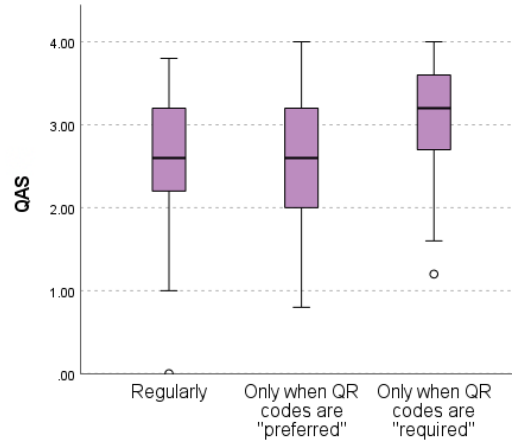

Fig. 3. QAS Score Distribution Per QR Code Usage

4.3   Quishing Implications

Our first research question asked for the susceptibility factors that contribute in a plausible quishing campaign for harvesting credentials. We did not harvest actual credentials as that constitutes more than a minimal harm to our participants, but we were able to determine the factors driving participants' willingness to yield credentials to a quishing website, nonetheless. Convenience, perhaps unsurprisingly, is the main factor contributing in successful quishing as 55.5% of the participants took the route of least resistance for transfer of credentials. The perception of online safety seems a promising factor that helped 11.5% of the participants to avoid yielding their Facebook/Google credentials, but we uncovered a worrisome trend of differential perception between Facebook (less safe) and Google (more safe) in 7.5% of the cases that still renders users susceptible to quishing.

Another ameliorating factor against quishing could be the reluctance to use Facebook/Google credentials by another 7.5% of the participants that opted to create a new account, but users tend to reuse credentials so quishers might still be able to harvest useful information [56]. Distrusting social media again could wield some anti-quishing leverage for users, but 4/5 of the 11.5% of participants that cited this factor chose to use their Google credentials. The most worrisome finding of our study, at least in the nascent stages of quishing, is that only 3.4% of the participants were suspicious of deception for credential harvesting.

It appears that crafting an authoritative pretext is still a sufficiently potent persuasion factor, regardless of the shift in phishing modality from an email to a QR code [41]. Quishing, similarly as its older sibling phishing, appears to thrive in conditions of scarcity as the requirements for proof-of-vaccination proved influential in increasing the credibility of the quishing pretext [55]. The social proof and reciprocation were perhaps less salient persuasion factors, but we did not

find any evidence explicitly countering their effect. One could argue that the considerable COVID-19 anti-vaccination sentiment [59] could render all persuasion factors unusable in the particular quishing context and that certainly is a line of future inquiry we want to pursue.

The lack of quishing awareness also worked to the advantage of the quishers in our study, as we also employed the QAS scale to answer the second research question. With an overall average score across the sample of $\overline{QAS} = 2.68, \sigma = 0.78$, only the participants that selected to skip the sign-up citing the convenience factor had scored higher on average. We saw the same outcome when considering the perceived safety as a factor with an exception of a +.04 in the average score of the participants that selected to sign-in with their Google credentials. The QAS scores associated with the reluctance of using Google/Facebook credentials and distrust in Facebook are on par or higher with the sample average, revealing a positive awareness of phishing and online deception in general. The suspicious participants, except the one choosing Facebook, scored .37 and .52 higher than the average when choosing a new account or skipping registration.

Quishing awareness is related to the frequency one uses QR codes as revealed by our analysis. As show in Figure 3, participants that used QR codes regularly or preferred them over other options for information transfer scored lower on the QAS scale compared to the ones that used QR codes only when required. The latter ones, however, constituted only 11.6% of our sample. Interestingly, only 15% of the participants chose to skip the registration, yielding only 1.7% of the sample entirely insulated from quishing by avoiding using QR codes and transferring credentials online. These findings reveal that quishing is a relevant threat given that users embrace or have no objection to the adaptation of QR code-based interaction imposed by the COVID-19 pandemic. Whether these results will hold in future certainly depends on how the adoption of QR codes will unfold and we are equally interested in exploring any induced shift in quishing.

5 ANTI-QUISHING

Changing users' behavior around potentially malicious QR codes was the imperative of our third and forth research questions, considering the surge in quishing attacks. As is the case with anti-phishing, the two logical approaches would be to: (1) train users how to spot a quishing campaign; and (2) develop security indicators within the QR code interaction elements to help users avoid falling for quish [73]. Phishing training is usually delivered through facts-and-advice materials [73], gamification or simulation for malicious URL detection [12, 66, 77] or embedded phishing exercises [67]. We certainly could not develop them all at once; instead, we contextualized each training modality to fit in a quishing setting in subsection 5.1. More practically, we propose several designs for quishing-appropriate security indicators in subsection 5.2 utilizing the previous work in security cues, warnings, and anti-phishing nudges [27, 62, 63, 70].

5.1 Quishing Awareness Training (RQ3)

QR codes apply in a wider range of information transfer that many phishing "trainees" might have not yet encountered. Take for example the most recent release of the Coinbase QR Code commercial at the Super Bowl LVI [42]. For most of the 60 second commercial block, users saw a black background with a QR code (in multiple monochrome colors) bouncing from corner to corner reminiscence of old screensavers (in the last moment, the commercial invited viewers to "Get $15 in free Bitcoin for signing up. Plus, a chance to win $3 million prizes!"). A deliberate choice to turn a legitimate QR code suspicious probably makes marketing sense by working on viewers' curiosity and reciprocity, but creates a confusing experience for users accustomed to paper QR codes for menus or electronic QR codes for movie tickets.

The facts-and-advice "stories" should therefore not just convey lessons but also cover quishing pretexts in detail. The lessons themselves are similar to the ones for phishing [73] and be logically adopted as a foundation in a basic quishing training. We propose one such adaptation in Table 4. The lessons fit well with our COVID-19 digital passport trial and

could equally materialize in a pretext where a victim is sent a legitimate link to a video resembling the commercial above where the QR code leads to an attacker-controlled cryptocurrency website with a more lucrative deal (usually clustered with cryptocurrency scams [58]).

Table 4. Facts-and-Advice Quishing Training: Basic Lessons

#	Lesson
1	Malicious QR codes resemble QR codes from restaurants, posters, or parking meters, but could also be attached in IT department emails, shown on websites and social media platforms, or even TV commercials
2	Read the link in the notification after scanning a QR code to see where it really goes to
3	If you click a link right after scanning a QR code, your identity can be stolen
4	If you click a link after scanning a QR code, make sure to look for security indicators preceding the URL in the browser like 'Not Secure' tags, exclamation marks, strike-through words or padlock icons, or red warning screens
5	Malicious QR codes enable 'quishing' or phishing with QR codes. Phishing is when an attacker sends you a fake email; Quishing is when an attacker gets you scan a fake QR code
6	Quishing is your problem because if you click on the link after scanning a fake QR code, it is your information being stolen

The myriad of quishing pretexts and the nature of QR code interactions make a more convincing case for a training delivered through gamification. Traditional phishing training is usually delivered online (e.g. a gaming website or an app). QR codes allow for extending the game in physical spaces, akin to alternate reality games (ARGs) [29]. QR codes could easily enable application of the *reflection* game design principle [12] where "players" stop and reflect after encountering and scanning such a code, e.g. a QR code sticker over a regular billboard or a QR code icon bouncing from corner to corner on a digital billboard at a bus stop. QR codes also fit with the *story-based agent environment* principle - a "player" doesn't have to be a "fish" but could be a "papparazzi" agent scanning QR codes around exclusive places, for example. Or become a "forensic investigator" agent looking for both physical and URL tampering of QR codes, as in other security-related ARGs [49]. Since quishing is a form of phishing, the *conceptual–procedural* principle is easy to satisfy with facts-and-advice procedural phishing knowledge and iteratively build the concept of malicious QR codes.

ARGs are versatile enough to extend the embedded phishing exercises usually applied in working environments [67]. Employees could be periodically "quished" with emails containing malicious codes as in [19], but an ARG could help employees' retain and expand their general phishing knowledge. An ARG with posters including training QR codes in common rooms, company's parking garages, or even collaborative platforms like Slack could increase both quishing and phishing awareness over a longer period of time, provided that measures based interactive examples perform best in reminding employees about online deception [64]. QR codes are low-cost extension of the general phishing awareness training and companies could also capitalize on their internal adaptations to accommodate QR codes since the COVID-19 pandemic start.

5.2 Quishing Security Indicators (RQ4)

In our study, only participant **P123** noticed the security indicator preceding the malicious URL. Evidence suggests that users' often find security indicators confusing and irrelevant [63]. Users also "habituate" to repetitive exposure or security warnings online [70]. To rectify this problem, security indicators deliberately include "design frictions" designed to disrupt automatic interactions, and grab the attention of the users [21]. Following this approach, we developed four possible security indicators to grab users' attention when scanning QR codes, shown in Figure 4. All four security indicators use the standard browser warning heading "Deceptive Website Warning" and follow up text regularly shown
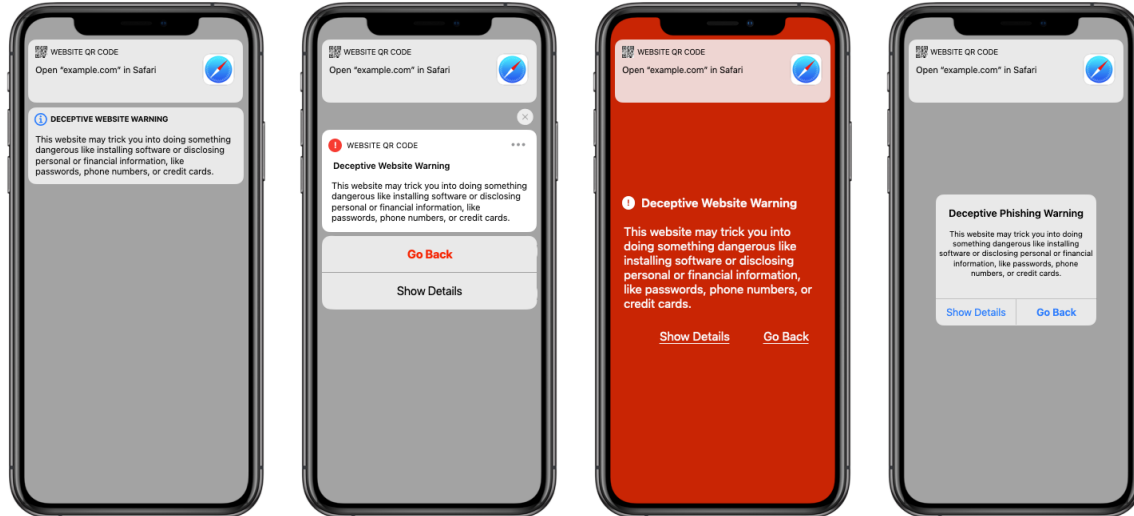
Fig. 4. Quishing Security Awareness Indicators: (a) additional notification; (b) extended notification with actions; (c) background screen with actions; (d) alert with actions

when users encounter suspected websites in Safari [5]. We use an visual/action-based inhibitors in variable degrees during the user QR code interaction to meet a wider range of user preferences for security warnings [74].

The first security indicator (A) is a simple notification after the standard notification users receive when scanning a QR code. Here, we employ minimal yet meaningful visual friction with an indicator that contains a blue information icon and blends with the notification structure in iOS. The second security indicator (B) increases the visual friction with the red exclamation icon attached to application tiles in iOS and offers the possibility for a user to take either a "Go Back" or "Show Details" actions. The third security indicator (C) maximizes the visual friction by displaying a standard red browser warning in the background over the entire screen with the same two action options. The last security indicator instead uses the alert popup in iOS as an interaction friction to warn the user and explicitly demand either of the actions to be taken before the user proceeds.

We conducted a follow-up usability study with another sample of 124 participants where we tested each of the security indicator options. This study was also approved by the IRB of our institution. We recruited Amazon Mechanical Turk participants that were 18 years or above old, with iPhone as a primary mobile device, and have scanned QR codes with their iPhone to open URLs. The study was anonymous and took around 15 minutes to complete with the standard compensation rate. We first collected data to calculate their QAS scores, then exposed them to the concept of quishing and collected their preferences (up to two). The sample contained 44.4% female and 55.6% male participants. Most of them were college graduates (58.1%), followed by high school graduates (32.3%), post graduates (8.9%) and only 0.1% participants with less than a high school education. Age-wise, 44.4% were in the [35-44] bracket, 24.2% in [25-34], 12.9% in [45-54], 15.3% in [55-64], and 3.2% in [18-24].

Table 5 shows the distribution of the user preferences with the average QAS score and standard deviation for each choice. The security indicator (C) was the most preferred one by the participants that, interestingly, scored lower than the average QAS of the sample. The attention grabbing effect of the red screen was obvious and useful to participants:

"*It grabs your attention. Little boxes that look like every other notification often go unread and get clicked on haphazardly*" [**P61**]. Participants also preferred the security indicator (C) together with the security indicator (B), scoring a bit higher than the previous group, but still bellow the average QAS of the sample. Here, participants suggested what actually they would like to see as a security warning: "*Option B was my favorite because it offered me details. Option C I like because the red screen was very obviously something bad but it wasn't my first choice because I feel like it could be overly worrying for some people*" [**P35**]

The third most preferred security indicator was (B) and this group of participants scored the lowest of all groups on the QAS scale. Participants like this option because: "*It incorporates red, which I quickly associate with a problem. It doesn't crowd the screen. It has two action buttons easily accessible*" [**P7**]. The group of participants the scored the highest on the QAS scale preferred both the security indicator (B) and (D). They praised the balancing effort of visual frictions with explicit actions: *I think they're the most concise, and they look the most modern and less 'scary' than the other options. They seem the most normal, they feel familiar.*" [**P43**].

Participants preferred the security indicator (D) alone because: "*It provided enough details but also gave me a choice on how to continue*" [**P123**], or together with (C) because: "*Those two are much more emphatic in letting me know to be suspicious. If a user is distracted or just not thinking 100% through their process, the other warnings might not be emphatic enough to grab their attention* [**P121**]. The participant that chose the security indicator (D) together with (A) disliked the red color and the one preferring the security indicator (A) stated: "*I would rather make the choice myself on what to do instead of being blocked completely*" [**P2**].

Table 5. Security Indicators Preferences

Preference	Count	$\overline{QAS}$	σ
A	1	2.2	/
A and D	1	2.4	/
B	17	2.33	.647
B and C	21	2.52	.601
B and D	5	2.92	.228
C	74	2.39	523
C and D	3	2.60	.6
D	2	2.50	.424
Total	**124**	**2.6**	**.584**

Only nine participants confirmed they encountered suspicious QR codes in the past with the second highest quishing awareness score ($\overline{QAS}$ = 2.80, σ = .435). Three of them cited they received QR codes via an instant message requesting bill payments to be submitted to the embedded URL, couple of them pointed to QR codes associated with cryptocurrencies, and the rest refereed to physical QR codes. Four of them explicitly stated they suspected the resulting website because of a security indicator associated with it: "*I clicked the QR code link that took me to a 'spammy' looking website that resulted in security warnings on my phone.*" [**P93**].

Controlling for QR code pattern of usage, 14.4% of the participants indicated they use QR codes regularly and preferred the security indicator (C) the most. This group scored the lowest on average on the QAS scale of all groups: $\overline{QAS}$ = 2.22, σ = .508. The 16% of the participants that preferred touch-free information transfer weren't much better on the QAS scale, scoring $\overline{QAS}$ = 2.29, σ = .412, but they were roughly evenly split between the preference for the security indicator (C) and (B). The remaining 59.6% of the participants that used QR codes only when required scored

the highest between the three usage groups on average: $\overline{QAS} = 2.52, \sigma = .568$. The preferences of this group were similarly distributed as in Table 5.

Controlling for gender identity, we noticed that the female participants preferred the security indicator (B) alone, and together with (D), more than the male participants ($\overline{QAS} = 2.40, \sigma = .494$). The male participants were overwhelmingly in support of the individual security indicator (C) and together with the other three options ($\overline{QAS} = 2.47, \sigma = .589$). Respective to the level of education, we noticed that the post-graduate degree participants overwhelmingly preferred the security indicator (C), while the other participants were more balanced in their preferences. Interestingly, they scored the lowest on QAS scale ($\overline{QAS} = 2.35, \sigma = .629$). Age-wise, the older the participants were, the more the stronger the preference of the individual indicator (C). Similarly, the QAS score decreased with the age, with the [18-24] bracket the highest ($\overline{QAS} = 2.85, \sigma = .1$).

6 DISCUSSION

Our quishing study uncovered important field evidence about this emerging type of phishing. The level of quishing susceptibility that we observed is on par or higher than the one for phishing, but this is perhaps to be expected given the early days of mass quishing [34]. People's vigilance, or the ability to detect anomalies for a sustained period, has been poor when it comes to phishing, so it is hardly probable for a positive change to happen when dealing with malicious QR codes [11, 72]. This is inline with the evidence that the majority of our participants readily trumped convenience over security. Even more, almost 60% of the participants in the follow-up study chose security indicator (C) which visually stands out the most, reasoning that a stronger friction is needed to turn their attention towards a potential anomaly with the embedded URL [9]. These two groups had lower-than-average QAS score, suggesting that QR code are seldom associated with anomalies or even negative consequences of clicking the embedded URL [34].

Our findings also points out a small but important set of suspicious users showing a proto-vigilance to quishing. Scoring among the highest on the QAS scale in both the main and the follow up study, these participants modeled their QR code behavior from what they know about or previously experienced with phishing, but rarely utilized security indicators. This probably results more from *neuroticism* or the anxious resistance to sharing information rather than from *conscientiousness* or attention to detail, the two personality traits associated with resistance to phishing [75].

Our follow-up usability study suggests that quishing is aided by poor cost/benefit trade-off for heeding security indicators [68]. First, a minute spent examining an URLs results in an estimated cost (in terms of user time) of two orders of magnitude greater than all phishing losses [36]. Second, the cost of learning the meaning of a security indicator outweighs the benefit of seamless interaction [63], Third, the cost of phishing losses, e.g. compromised credentials, seems to decrease, as few of participants put it: "*I don't mind having my Facebook login compromised, I can always reset the password.*" The time spent on scanning a QR code, on the other hand, is an acceptable cost and perhaps the security indicators should factor the temporal trade-off when warning about quishing [41].

6.1 Limitations

We note several limitations of our study. Repeating the study with a larger sample will add more evidence not just about the evolution of the quishing pretexts and tactics, but also provide further validation of the QAS scale. We used a COVID-19 pretext but future studies could uncover variable degrees of susceptibility to quishing moderated by new pretexts and overall increase in quishing awareness. We did not harvested actual credentials and it is plausible that many of the participants would have avoided the sign-up when encountering the impersonated Facebook and Google websites. We used iOS for quishing security indicators and users of other mobile operating systems might express

preferences that do not conform with the trend observed in our follow-up study. It is equally plausible that new and enhanced quishing indicators will be developed in future that would render the ones proposed in this study obsolete.

Our participants were 18 years or older and from the US. However, smartphones are prevalent among teenagers [4] and they also encounter QR codes on increased basis (e.g. scavenger hunts [35]). Our results might not entirely generalize for age groups below 18 years given their specific smartphone usage patterns [2], despite the fact that teenagers show poor performance in detecting phishing [53]. Similar limitation holds for users' country of residence as phishing susceptibility differs from country to country [33]. We also acknowledge that users might entirely abandon a login prompt after scanning a QR code, a valid real-world case to which our results do not apply (we did not collect data for this case in our study).

We used simple QR codes in our study, however, the beautification of QR codes is an active area of development where images, dimensions, or reflection effects are incorporated to further personalize the layouts [76]. All of these factors could affect how a user approaches to scan a QR code in a first place and access the embedded URL for potential quishing. We also performed the study when no considerable proposal for creating a secure QR code ecosystem exists. Novel security primitives for QR codes and regularly updated lists of quishing URLs and domains for automated quishing detection could make future quishing difficult [1].

6.2 Ethical Considerations

Every public phishing study runs the risk of informing the real-world phishers about the actionable anti-phishing plans. Our study is no exception and we are aware that the preliminary results suggesting high level of susceptibility and relatively low quishing awareness could amplify the quishing attacks in the wild. We believe, however, that the benefits of this field study significantly outweigh the potential quishing harm, especially our actionable proposals for anti-phishing training and security indicators. One could object that the COVID-19 vaccination pretext might have negative consequences in dissuading users against getting a vaccine and thus undermine the collective mass immunization effort. We did not observe such an effect and we could not control how each reader internalizes our findings. Phishers already employ COVID-19 as a pretext at large for some time [15], so our study should not tip the vaccination scales considerably.

7 CONCLUSION

Quishing is as much of a real issue as its big brother phishing. As in phishing, individuals are willing to compromise credentials for the sake of convenience when accessing malicious URL embedded in QR codes. Individuals do lack quishing awareness, but unlike phishing, neither training nor advice is readily available yet. We took the opportunity to develop a scale to measure the quishing awareness and use the results to create phishing training guidelines and test quishing security indicators. We hope that our results will help the security community towards an actionable anti-quishing effort that incorporates some of the suggested anti-quishing efforts.

REFERENCES
[1] Bhupendra Acharya and Phani Vadrevu. 2021. PhishPrint: Evading Phishing Detection Crawlers by Prior Profiling. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, 3775–3792. https://www.usenix.org/conference/usenixsecurity21/presentation/acharya

[2] Zinaida Adelhardt, Stefan Markus, and Thomas Eberle. 2018. Teenagers' Reaction on the Long-Lasting Separation from Smartphones, Anxiety and Fear of Missing Out. In *Proceedings of the 9th International Conference on Social Media and Society* (Copenhagen, Denmark) *(SMSociety '18)*. Association for Computing Machinery, New York, NY, USA, 212–216. https://doi.org/10.1145/3217804.3217914

[3] Mohamed Alsharnouby, Furkan Alaca, and Sonia Chiasson. 2015. Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies* 82 (2015), 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005

[4] Ionut Andone, Konrad Błaszkiewicz, Mark Eibes, Boris Trendafilov, Christian Montag, and Alexander Markowetz. 2016. How Age and Gender Affect Smartphone Usage. In *Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct* (Heidelberg, Germany) *(UbiComp '16)*. Association for Computing Machinery, New York, NY, USA, 9–12. https://doi.org/10.1145/2968219.2971451

[5] Apple. 2021. Safari & Privacy. https://www.apple.com/legal/privacy/data/en/safari/.

[6] Luke Barr. 2022. FBI warns criminals are using fake QR codes to scam users. https://abcnews.go.com/Politics/fbi-warns-criminals-fake-qr-codes-scam-users/story?id=82371866.

[7] Lujo Bauer, Cristian Bravo-Lillo, Elli Fragkaki, and William Melicher. 2013. A Comparison of Users' Perceptions of and Willingness to Use Google, Facebook, and Google+ Single-Sign-on Functionality. In *Proceedings of the 2013 ACM Workshop on Digital Identity Management* (Berlin, Germany) *(DIM '13)*. Association for Computing Machinery, New York, NY, USA, 25–36. https://doi.org/10.1145/2517881.2517886

[8] Mark Blythe, Helen Petrie, and John A. Clark. 2011. F for Fake: Four Studies on How We Fall for Phish. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Vancouver, BC, Canada) *(CHI '11)*. Association for Computing Machinery, New York, NY, USA, 3469–3478. https://doi.org/10.1145/1978942.1979459

[9] Cristian Bravo-Lillo, Saranga Komanduri, Lorrie Faith Cranor, Robert W. Reeder, Manya Sleeper, Julie Downs, and Stuart Schechter. 2013. Your Attention Please: Designing Security-Decision UIs to Make Genuine Risks Harder to Ignore. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (Newcastle, United Kingdom) *(SOUPS '13)*. Association for Computing Machinery, New York, NY, USA, Article 6, 12 pages. https://doi.org/10.1145/2501604.2501610

[10] Casey Canfield, Alex Davis, Baruch Fischhoff, Alain Forget, Sarah Pearman, and Jeremy Thomas. 2017. Replication: Challenges in Using Data Logs to Validate Phishing Detection Ability Metrics. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 271–284. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/canfield

[11] Casey Inez Canfield, Baruch Fischhoff, and Alex Davis. 2016. Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *Human Factors* 58, 8 (2016), 1158–1172. https://doi.org/10.1177/0018720816665025 PMID: 27562565.

[12] Gamze Canova, Melanie Volkamer, Clemens Bergmann, and Roland Borza. 2014. NoPhish: An Anti-Phishing Education App. In *Security and Trust Management*, Sjouke Mauw and Christian Damsgaard Jensen (Eds.). Springer International Publishing, Cham, 188–192.

[13] Fiona Carroll. 2021. *Usable Security and Aesthetics: Designing for Engaging Online Security Warnings and Cautions to Optimise User Security Whilst Affording Ease of Use.* Association for Computing Machinery, New York, NY, USA, 23–28. https://doi.org/10.1145/3481357.3481376

[14] Centers for Disease Control (CDC). 2019. Resuming Business Toolkit. https://www.cdc.gov/coronavirus/2019-ncov/community/resuming-business-toolkit.html.

[15] Centers for Disease Control (CDC). 2021. COVID-19-Related Phone Scams and Phishing Attacks. https://www.cdc.gov/media/phishing.html.

[16] Centers for Disease Control (CDC). 2021. Getting Your CDC COVID-19 Vaccination Record Card. https://www.cdc.gov/coronavirus/2019-ncov/vaccines/vaccination-card.html.

[17] Centers for Disease Control (CDC). 2021. Guidance for COVID-19. https://www.cdc.gov/coronavirus/2019-ncov/communication/guidance.html.

[18] Centers for Disease Control (CDC). 2021. Toolkit for General Public. https://www.cdc.gov/coronavirus/2019-ncov/communication/toolkits/general-public.html.

[19] Rachelle Chouinard. 2021. New Quishing Campaign Shows How Threat Actors Innovate to Bypass Security. https://abnormalsecurity.com/blog/qr-code-campaign-bypass-security.

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

[21] Anna L. Cox, Sandy J.J. Gould, Marta E. Cecchinato, Ioanna Iacovides, and Ian Renfree. 2016. Design Frictions for Mindful Interactions: The Case for Microboundaries. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI EA '16)*. Association for Computing Machinery, New York, NY, USA, 1389–1397. https://doi.org/10.1145/2851581.2892410

[22] Adrian Dabrowski, Katharina Krombholz, Johanna Ullrich, and Edgar R. Weippl. 2014. QR Inception: Barcode-in-Barcode Attacks. In *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones and Mobile Devices* (Scottsdale, Arizona, USA) *(SPSM '14)*. Association for Computing Machinery, New York, NY, USA, 3–10. https://doi.org/10.1145/2666620.2666624

[23] Christopher Dye and Melinda C Mills. 2021. COVID-19 vaccination passports. *Science* 371, 6535 (2021), 1184–1184.

[24] Serge Egelman, Marian Harbach, and Eyal Peer. 2016. Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 5257–5261. https://doi.org/10.1145/2858036.2858265

[25] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 2873–2882. https://doi.org/10.1145/2702123.2702249

[26] Serge Egelman and Stuart Schechter. 2013. The Importance of Being Earnest [In Security Warnings]. In *Financial Cryptography and Data Security*, Ahmad-Reza Sadeghi (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 52–59.

[27] Adrienne Porter Felt, Robert W. Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. 2016. Rethinking Connection Security Indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 1–14. https://www.usenix.org/conference/soups2016/technical-sessions/presentation/porter-felt

[28] Ana Ferreira, Lynne Coventry, and Gabriele Lenzini. 2015. Principles of Persuasion in Social Engineering and Their Use in Phishing. In *Human Aspects of Information Security, Privacy, and Trust*, Theo Tryfonas and Ioannis Askoxylakis (Eds.). Springer, 36–47.

[29] Tanya Flushman, Mark Gondree, and Zachary N. J. Peterson. 2015. This is Not a Game: Early Observations on Using Alternate Reality Games for Teaching Security Concepts to First-Year Undergraduates. In *8th Workshop on Cyber Security Experimentation and Test (CSET 15)*. USENIX Association, Washington, D.C. https://www.usenix.org/conference/cset15/workshop-program/presentation/flushman

[30] Riccardo Focardi, Flaminia L. Luccio, and Heider A.M. Wahsheh. 2019. Usable security for QR code. *Journal of Information Security and Applications* 48 (2019), 102369. https://doi.org/10.1016/j.jisa.2019.102369

[31] Anjuli Franz, Verena Zimmermann, Gregor Albrecht, Katrin Hartwig, Christian Reuter, Alexander Benlian, and Joachim Vogt. 2021. 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, 339–358. https://www.usenix.org/conference/soups2021/presentation/franz

[32] Gerd Gigerenzer and Peter M Todd. 1999. Fast and frugal heuristics: The adaptive toolbox. In *Simple heuristics that make us smart*. Oxford University Press, 3–34.

[33] Shakthidhar Gopavaram, Jayati Dev, Marthie Grobler, DongInn Kim, Sanchari Das, and L Jean Camp. 2021. Cross-National Study on Phishing Resilience. In *Proceedings of the Workshop on Usable Security and Privacy (USEC)*.

[34] Frank L. Greitzer, Wanru Li, Kathryn B. Laskey, James Lee, and Justin Purl. 2021. Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility. *Trans. Soc. Comput.* 4, 2, Article 8 (jun 2021), 48 pages. https://doi.org/10.1145/3461672

[35] Julia Gressick, Bruce Alan Spitzer, and Kyle Sagarsee. 2014. Designing interactive scavenger hunt using QR codes. *Journal of Teaching and Learning with Technology* (2014), 90–93.

[36] Cormac Herley. 2009. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proceedings of the 2009 Workshop on New Security Paradigms Workshop* (Oxford, United Kingdom) *(NSPW '09)*. Association for Computing Machinery, New York, NY, USA, 133–144. https://doi.org/10.1145/1719030.1719050

[37] Tai-Wei Kan, Chin-Hung Teng, and Mike Y Chen. 2011. QR code based augmented reality applications. In *Handbook of augmented reality*. Springer, 339–354.

[38] Amin Kharraz, Engin Kirda, William Robertson, Davide Balzarotti, and Aurélien Francillon. 2014. Optical Delusions: A Study of Malicious QR Codes in the Wild. In *2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. 192–203. https://doi.org/10.1109/DSN.2014.103

[39] Peter Kieseberg, Sebastian Schrittwieser, Manuel Leithner, Martin Mulazzani, Edgar Weippl, Lindsay Munroe, and Mayank Sinha. 2012. *Malicious Pixels Using QR Codes as Attack Vector*. Atlantis Press, Paris, 21–38. https://doi.org/10.2991/978-94-91216-71-8_2

[40] Katharina Krombholz, Peter Frühwirt, Peter Kieseberg, Ioannis Kapsalis, Markus Huber, and Edgar Weippl. 2014. QR code security: A survey of attacks and challenges for usable security. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 79–90.

[41] Katharina Krombholz, Peter Frühwirt, Thomas Rieder, Ioannis Kapsalis, Johanna Ullrich, and Edgar Weippl. 2015. QR Code Security – How Secure and Usable Apps Can Protect Users Against Malicious QR Codes. (2015), 230–237. https://doi.org/10.1109/ARES.2015.84

[42] Gabe Lacques. 2022. What was that? Coinbase's QR code Super Bowl commercial confuses viewers. (2022). https://www.usatoday.com/story/sports/Ad-Meter/2022/02/13/coinbase-qr-code-super-bowl-ad-crypto-commercial-confuses-viewers/6778949001/.

[43] Yijie Li, Yi-Chao Chen, Xiaoyu Ji, Hao Pan, Lanqing Yang, Guangtao Xue, and Jiadi Yu. 2020. *Toward a Secure QR Code System by Fingerprinting Screens*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3372224.3418165

[44] Tian Lin, Daniel E. Capecci, Donovan M. Ellis, Harold A. Rocha, Sandeep Dommaraju, Daniela S. Oliveira, and Natalie C. Ebner. 2019. Susceptibility to Spear-Phishing Emails: Effects of Internet User Demographics and Email Content. *ACM Trans. Comput.-Hum. Interact.* 26, 5, Article 32 (July 2019), 28 pages. https://doi.org/10.1145/3336141

[45] Zane Ma, Joshua Reynolds, Joseph Dickinson, Kaishen Wang, Taylor Judd, Joseph D. Barnes, Joshua Mason, and Michael Bailey. 2019. The Impact of Secure Transport Protocols on Phishing Efficacy. In *12th USENIX Workshop on Cyber Security Experimentation and Test (CSET 19)*. USENIX Association, Santa Clara, CA. https://www.usenix.org/conference/cset19/presentation/ma

[46] Hugo Martin. 2021. COVID vaccine 'passports' in the U.S.: Here's what we're getting and why. https://www.latimes.com/business/story/2021-06-14/covid-vaccine-passport-united-states.

[47] Vasileios Mavroeidis and Mathew Nicho. 2017. Quick Response Code Secure: A Cryptographically Secure Anti-Phishing Tool for QR Code Attacks. In *Computer Network Security*, Jacek Rak, John Bay, Igor Kotenko, Leonard Popyack, Victor Skormin, and Krzysztof Szczypiorski (Eds.). Springer International Publishing, Cham, 313–324.

[48] René Mayrhofer and Stephan Sigg. 2021. Adversary Models for Mobile Device Authentication. *ACM Comput. Surv.* 54, 9, Article 198 (oct 2021), 35 pages. https://doi.org/10.1145/3477601

[49] John R. Morelock and Zachary Peterson. 2018. Authenticity, Ethicality, and Motivation: A Formal Evaluation of a 10-week Computer Security Alternate Reality Game for CS Undergraduates. In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*. USENIX Association, Baltimore, MD. https://www.usenix.org/conference/ase18/presentation/morelock

[50] María M. Moreno-Fernandez, Fernando Blanco, Pablo Garaizar, and Helena Matute. 2017. Fishing for phishers. Improving Internet users' sensitivity to visual deception cues to prevent electronic fraud. *Computers in Human Behavior* 69 (2017), 421–436. https://doi.org/10.1016/j.chb.2016.12.044

[51] Sean Murphy. 2021. Laravel QR Code Generator Infected with Malware. https://www.kernelmode.blog/laravel-qr-code-generator-infected-with-malware/.

[52] James Nicholson, Lynne Coventry, and Pam Briggs. 2017. Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. USENIX Association, Santa Clara, CA, 285–298. https://www.usenix.org/conference/soups2017/technical-sessions/presentation/nicholson

[53] James Nicholson, Yousra Javed, Matt Dixon, Lynne Coventry, Opeyemi Dele Ajayi, and Philip Anderson. 2020. Investigating teenagers' ability to detect phishing messages. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 140–149.

[54] Federal Bureau of Investigation. 2022. Cybercriminals Tampering with QR Codes to Steal Victim Funds. (Jan 2022). https://www.ic3.gov/Media/Y2022/PSA220118.

[55] Kathryn Parsons, Marcus Butavicius, Paul Delfabbro, and Meredith Lillie. 2019. Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies* 128 (2019), 17–26.

[56] Sarah Pearman, Shikun Aerin Zhang, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2019. Why people (don't) use password managers effectively. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA, 319–338. https://www.usenix.org/conference/soups2019/presentation/pearman

[57] Justin Petelka, Yixin Zou, and Florian Schaub. 2019. Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3290605.3300748

[58] Ross Phillips and Heidi Wilder. 2020. Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites. In *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. 1–8. https://doi.org/10.1109/ICBC48266.2020.9169433

[59] Samuel Pullan and Mrinalini Dey. 2021. Vaccine hesitancy and anti-vaccination in the time of COVID-19: A Google Trends analysis. *Vaccine* 39, 14 (2021), 1877–1881.

[60] Florian Quinkert, Martin Degeling, Jim Blythe, and Thorsten Holz. 2020. Be the Phisher – Understanding Users' Perception of Malicious Domains. In *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security* (Taipei, Taiwan) *(ASIA CCS '20)*. Association for Computing Machinery, New York, NY, USA, 263–276. https://doi.org/10.1145/3320269.3384765

[61] Elissa M. Redmiles. 2019. "Should I worry?" A Cross-Cultural Examination of Account Security Incident Response. In *2019 IEEE Symposium on Security and Privacy (SP)*. 920–934. https://doi.org/10.1109/SP.2019.00059

[62] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L. Mazurek. 2020. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, 89–108. https://www.usenix.org/conference/usenixsecurity20/presentation/redmiles

[63] Robert W. Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. 2018. *An Experience Sampling Study of User Reactions to Browser Warnings in the Field*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3173574.3174086

[64] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana von Landesberger, and Melanie Volkamer. 2020. 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, 259–284. https://www.usenix.org/conference/soups2020/presentation/reinheimer

[65] Filipo Sharevski and Peter Jachim. 2021. Alexa in Phishingland: Empirical Assessment of Susceptibility to Phishing Pretexting in Voice Assistant Environments. In *2021 IEEE Security and Privacy Workshops (SPW)*. 207–213. https://doi.org/10.1109/SPW53761.2021.00034

[66] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, USA) *(SOUPS '07)*. Association for Computing Machinery, New York, NY, USA, 88–99. https://doi.org/10.1145/1280680.1280692

[67] Hossein Siadati, Sean Palka, Avi Siegel, and Damon McCoy. 2017. Measuring the Effectiveness of Embedded Phishing Exercises. In *10th USENIX Workshop on Cyber Security Experimentation and Test (CSET 17)*. USENIX Association, Vancouver, BC. https://www.usenix.org/conference/cset17/workshop-program/presentation/siadatii

[68] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying wolf: An empirical study of ssl warning effectiveness.. In *18th USENIX Security Symposium (USENIX Security 09)*. USENIX Association, 399–342. https://www.usenix.org/event/sec09/tech/full_papers/sec09_browser.pdf

[69] Christopher Thompson, Martin Shelton, Emily Stark, Maximilian Walker, Emily Schechter, and Adrienne Porter Felt. 2019. The Web's Identity Crisis: Understanding the Effectiveness of Website Identity Indicators. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA, 1715–1732. https://www.usenix.org/conference/usenixsecurity19/presentation/thompson

[70] Anthony Vance, David Eargle, Jeffrey L. Jenkins, C. Brock Kirwan, and Bonnie Brinton Anderson. 2019. The Fog of Warnings: How Non-essential Notifications Blur with Security Warnings. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. USENIX Association, Santa Clara, CA. https://www.usenix.org/conference/soups2019/presentation/vance

[71] Timothy Vidas, Emmanuel Owusu, Shuai Wang, Cheng Zeng, Lorrie Faith Cranor, and Nicolas Christin. 2013. QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. In *Financial Cryptography and Data Security*, Andrew A. Adams, Michael Brenner, and Matthew Smith (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 52–69.

[72] Rick Wash. 2020. How Experts Detect Phishing Scam Emails. *Proc. ACM Hum.-Comput. Interact.* 4, CSCW2, Article 160 (oct 2020), 28 pages. https://doi.org/10.1145/3415231

[73] Rick Wash and Molly M. Cooper. 2018. *Who Provides Phishing Training? Facts, Stories, and People Like Me.* Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3173574.3174066

[74] Michael S Wogalter, Vincent C Conzola, and Tonya L Smith-Jackson. 2002. based guidelines for warning design and evaluation. *Applied ergonomics* 33, 3 (2002), 219–230.

[75] Michael Workman. 2008. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology* 59, 4 (2008), 662–674.

[76] Mingliang Xu, Qingfeng Li, Jianwei Niu, Hao Su, Xiting Liu, Weiwei Xu, Pei Lv, Bing Zhou, and Yi Yang. 2021. ART-UP: A Novel Method for Generating Scanning-Robust Aesthetic QR Codes. *ACM Trans. Multimedia Comput. Commun. Appl.* 17, 1, Article 25 (apr 2021), 23 pages. https://doi.org/10.1145/3418214

[77] Weining Yang, Aiping Xiong, Jing Chen, Robert W. Proctor, and Ninghui Li. 2017. Use of Phishing Training to Improve Security Warning Compliance: Evidence from a Field Experiment. In *Proceedings of the Hot Topics in Science of Security: Symposium and Bootcamp* (Hanover, MD, USA) *(HoTSoS)*. Association for Computing Machinery, New York, NY, USA, 52–61. https://doi.org/10.1145/3055305.3055310

[78] Anfu Zhou, Guangyuan Su, Shilin Zhu, and HuaDong Ma. 2019. Invisible QR Code Hijacking Using Smart LED. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 3, 3, Article 126 (Sept. 2019), 23 pages. https://doi.org/10.1145/3351284