Investigating University QR Code Interactions

Jeremiah D. Still, Thomas Morris, and Morgan Edwards

Old Dominion University, Norfolk, VA 23508, USA
{jstill | tmorr001 | mthom122}@odu.edu

Abstract. Although engaging with Quick Response (QR) codes presents a security risk, little observational data exists exploring the impact of informational cues on engagement. While naturalistic observations of on and off-campus QR code engagement by Vidas et al. (2013) demonstrated that curiosity instead of informational-driven needs motivate engagement, it seems informational cues should play a role in security-based decisions. Over a decade later, our study investigates naturalistic engagement with QR codes on campus with a focus on flyer informational cues. The flyers were placed in busy campus areas and regularly checked for visibility by research assistants. We captured the number of users engaging with the QR code by flyer type (i.e., blank, university logo only, phishing job ad). Study participants were asked to complete a brief survey sharing their security experience, motivations, and predicted future behavior. Our flyer engagement was low, similar to Vidas et al. (2013), particularly considering the size of our campus student population. We showed that the engagement across the flyer types increased as informational cues increased. It is encouraging to see low engagement, given these suspicious flyers. This shift towards information seeking over simple curiosity most likely reflects users' greater awareness of QRishing attacks.

Keywords: Cybersecurity, Human Factors, Phishing.

1 QR Codes: Human-Centered Cybersecurity

End-users often overestimate their cybersecurity expertise and capabilities [1]. Users often lack the cybersecurity knowledge and means to protect themselves. As technological systems from work and home computing environments merge [2], impacted assets from a security breach can be both personal and organizational. A lack of situational awareness can carry significant costs for our economy. Maintaining an appropriate amount of knowledge is difficult as technology quickly evolves. We recently saw a societal increase in Quick Response (QR) code usage - especially in marketing. It even made for a memorable Super Bowl ad in 2022 [3]. Coinbase had a sixty-second ad showing only a colorful QR code moving across the television screen. Coinbase engaged their audience by drawing on their curiosity [4, 5]. QR codes hide their target in a visual code. Those square matrix barcodes allow us to access websites, offers, and coupons. Historically, they are used to allow easy website access, but barriers initially slowed widespread adoption. Now, most cellular phones have camer-

as, the code is easy to manufacture, and, as a result, QR codes have been adopted in numerous industries [6, 7]. Global QR code usage has quadrupled from 2022 to 2023 [8]. The most popular usage includes URLs (46%), files (31%), vCards (7%), and social media links (4%). The pandemic brought QR codes back to the forefront through the use of contactless payments, menus, and check-ins [8]. This growth has increased phishing attacks [9].

Phishing is defined as an act of deception intended to steal a person's private information. Conventionally, we think of phishing attacks as when someone sends you an e-mail posing as a legitimate source (e.g., their bank) to gain access to your personal data (e.g., bank account information). These attacks can lead to monetary and privacy losses for unsuspecting users. Phishing attacks are social engineering attacks [10, 11], because they focus on exploiting the human element instead of a technical hack. Cyber defenders introduced security indicators meant to help prevent end-users from falling victim to browser phishing, but the indicators still failed to offer significant protection [12, 13]. For example, Alsharnoby, Alaca, and Chiasson (2015) showed only 53% of phishing websites were detected even when participants were primed to identify them. Along similar lines, it was found that users spent very little time looking at the security indicators. Historically, phishing attacks have taken the form of webpages or emails; however, in recent years, new forms of this attack are gaining in popularity [15]. For instance, QR codes can be deployed by attackers in public areas. For example, malicious QR codes have been planted near or onto parking meters, which drivers typically scan during the parking payment process. If the wrong QR code is scanned, their payment information and login credentials are stolen through a counterfeit website [9]. It is challenging to prevent hijacking attacks as QR codes are used on a massive scale and they are scanned in uncontrolled environments [16]. Therefore, we must depend on users' ability to identify a QRishing attack. For example, in the parking payment process, users should check for stickers placed over existing QR codes. Similarly, users should pause and search for trustworthy informational cues (e.g., branding and the appropriateness of content given the surroundings) before scanning a QR code.

2 End User Vulnerability & Risk Mitigation

QR codes give users an efficient way to access URLs and files on mobile devices by preventing the need to type long addresses. They are familiar to the public and employed in contexts that are high stakes (e.g., providing personal information during a hotel check-in). Unfortunately, hackers are using the platform maliciously [17]. Whether the attackers are covering a legitimate QR code or planting a QR code, users are becoming victims of cyber-attacks. According to ReliaQuest's report (2023), QR code attacks increased 51% between January and August. They claim this increase in attacks is due to the prevalence of phones with QR code scanners and due to users interacting with those codes without consideration of authenticity.

To mitigate risk, users must understand how a QR code can be malicious. It can send users to compromised websites to install malware, present them with a fake log-

in page, or exploit a software bug to infect their phone. Next, they need to know what to do before scanning a QR code to help mitigate risk. Users need to determine whether the QR code in the sticker or flyer form is trustworthy. For example, does the flyer contain enough informational cues to judge trustworthiness? Making a good decision requires you to check the surface for modifications (i.e., sticker covering the original QR code), consider the creator (i.e., do you know them), and the genuineness of the flyer. Similar to e-mail and website phishing attacks, end-users should look for red flags.

Kumar et al. (2022) surveyed end-users of QR codes and found that more than half had safety concerns when using a QR code. They reported looking for informational cues like brand logos or QR codes with higher pixel density and larger sizes. Unfortunately, over one-third of those surveyed reported no concern for their safety during QR code usage. It appears many users are aware of threats associated with QR code usage and are looking for cues to determine trustworthiness.

Over a decade ago, Vidas et al. (2013) examined some aspects of how user engagement is impacted by informational cues. They posted over one hundred QR flyers in public locations in Pittsburgh, Pennsylvania. Three types of flyers were employed: 1. QR code only (with and without usage instructions) 2. QR code with research study recruitment information 3. Rip-off tabs only without QR code for the same research recruitment information. Across four weeks, 61% of the flyers had been scanned by at least one person. Notably, most of the users (i.e., 75%) stated they scanned the QR code out of curiosity. They found that few wanted to learn more about the flyers' content. To further support this perspective, they found that as informational cues increased, engagement decreased. That is, viewers were more likely to visit the URL associated with the QR code only than the QR code surrounded by research study recruitment information. Vidas et al. (2013) also performed a follow-up surveillance study on their university campus to examine how many viewers subsequently scanned the QR code and continued to the target URL. They provided evidence that most users scanning a QR code (i.e., 85%) continue to the URL.

We investigated the usage of QR codes in a naturalistic setting similar to Vidas et al. (2013) but focused on the impact of informational cues on engagement. We examined: 1) How often university students scan QR codes on flyers and 2) Whether engagement would be impacted by informational cues on QR code flyers. We used three flyer designs: blank, university logo, and fake job ad. The blank flyer only showed the QR code. Given the lack of any informational cues, this QR code should not be scanned. The QR code with the university logo was expected to create some trustworthiness by association with a trusted brand (c.f., Kumar et al, 2022). Finally, the fake job ad was intended to create the most trust; it aligned the message with the surrounding context, and the flyer showed the name of the supposed creator. Because it was a fake ad, the name on the ad, Dr. Amy Miller, was not an employee of the university, but the content of the ad - seeking student help and offering flexible scheduling - seems to be a conventional message for a university campus. We predicted that engagement would increase as informational cues on the paper flyers increased.

3. Studying University QR Interactions

3.1 Addressing Ethical Concerns

To accomplish the research aims of this study, data had to be collected in the real world. Collecting naturalistic QR code usage behavior in a traditional laboratory environment is impossible. According to the university IRB, we had two ethical concerns to address with this study. First, the design is not a conventional naturalistic observation; it is a contrived observation because the flyers were placed in the environment for the express purpose of this study, and we manipulated the flyer design. Although the aim of the study was to examine factors that contribute to risky QR code use, it was important to provide standard protections for participants as well as to provide more immediate positive outcomes for participants. To this end, participants' data remained anonymous. No unique identifying visitor information was recorded for those who used the QR code and technical data that was collected from the encounter (e.g., browser, OS, screen resolution, geographic region) was described to the participant. The PI's contact information was provided for those who had further questions. In addition to this, participants were provided with guidance for safe QR code practices. This is the first paragraph they encountered:

> QR codes direct you to a link you may not be able to see. Due to this, it is important that you only scan QR codes when it is necessary and when you have taken the time to decide if the QR code should be trusted. This is because sometimes people will use QR codes to redirect you to websites that aim to steal your information. If it is possible, try to preview the link the QR code sends you to before deciding to go to the link. Also, if possible, try searching online for the information or manually typing the website link instead of scanning the QR code. It is important that you slow down and consider not all QR codes will direct you to legitimate websites, even if the QR code appears in a legitimate location or expected location. For detailed information on QR code risks and remedies, please read the announcement created by ODU IT security and planning.

Following this introduction, they learned about the risks of using QR codes and how they can be used maliciously (e.g., cyber attackers can direct them to a fake login; attempt to collect personal information). They learned to protect themselves against malicious QR codes (e.g., never scan a QR Code from an untrusted source; check for stickers). At the end of the risks and remedies educational piece, they were provided a URL to more cyber security and information security tips [21]. Finally, participants were asked to complete a follow-up five-question survey as part of the study or, if they were finished, to close the page. The IRB committee approved all stimuli and procedures.

3.2 Procedure

Three flyer designs varied the amount of informational cues available to the viewer and were distributed across campus. The flyers were posted on bulletin boards in the

student library, university student center, and engineering building for a duration of one week. After the week, the codes were moved to a new location. The order was counterbalanced, so after three weeks, all three QR codes were displayed once in each of the buildings. The QR code availability was reviewed every two to three days to ensure it was still visible on the bulletin board. The QR code would direct participants to Qualtrics when scanned. Participants were informed the QR code was part of a research study, and then a description of the associated risks of interacting with QR codes and recommendations for ways to limit risk were provided. Anonymous user data were collected, including viewing time, browser type, OS version, operating system, and screen resolution. Participants then had the option to respond to five survey questions: 1. Have you been trained in cybersecurity in the past? 2. Do you consider yourself a cybersecurity expert? 3. How concerned are you with cybersecurity? 4. How frequently do you plan to scan QR codes in the future? 5. What motivated you to scan this QR code?

3.3 Apparatus & Stimuli

Three flyer designs were created and printed: blank, with a university logo, and a fake job ad (taken from an e-mail Phishing example). The blank flyer had no additional information cues; it only showed the QR code (see Fig. 1). The QR code with the university logo was intended to have more credibility via association with a trusted brand (see Fig. 2). Finally, the phishing flyer for the fake job was created with the intent of aligning the QR code message with the surrounding university research context; to further increase credibility, it included the name of the supposed creator (see Fig. 3). Those who scanned a QR code flyer were directed to the Qualtrics platform where they had access to information about the study and had the option to complete the five-item survey.

Fig. 1. Blank QR Code Flyer

Fig. 2. QR Code with ODU Logo Flyer

Fig. 3. QR Code Phishing (Fake Job Ad) Flyer. The flyer addresses students and is signed by Dr. Amy Miller. The body of the message says, “We understand the needs and demands of a student’s schedule, so we offer flexible schedules that enable you to earn money weekly and keep up with your coursework and extracurricular activities. Scan this QR code and give me your Telephone number, major/minor and email address for more details”.

3.4 Participants

Our possible participants included anyone within our large university population located in the southeastern region of the United States of America (55% females: 18,678 undergraduate and 4,816 graduate enrollment) as well as visitors to campus. Twenty-two participants scanned the QR code flyers. The following anonymous user data were collected: browser type (Chrome: 8, Safari: 14), Phone Platform (Android: 8, iPhone: 14), Operating System (Android: 10-13; iPhone: 15-16), and screen resolution (360x760: 4, 385x854: 2, 390x844: 1, 412x869: 2, 414x896: 7, 428x926: 6).

4. Results

4.1 Viewing Time

Only two participants viewed the QR code Qualtrics information page for more than four seconds (i.e., 57 seconds and 110 seconds). These participants were associated with the university logo flyer (see Fig. 2). Those two participants were also the only ones who completed the five-question survey. The majority of the viewers bounced on page arrival (n = 17) in less than 2 seconds. The remaining participants only skimmed the landing page (n = 3) for less than 5 seconds.

4.2 Engagement by Flyer Type

The descriptive data clearly suggest that flyer informational cues increase engagement. Of the 22 user engagements, the blank flyer only got 18% engagement. Adding the university logo to the flyer captured 32%. While the phishing flyer for the fake job was the most effective, with 50 % of the overall engagement.

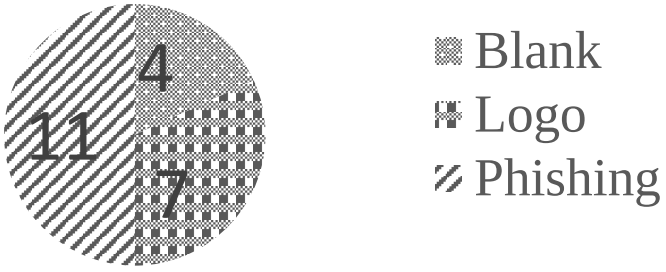

Fig. 4. This pie chart displays the number of interactions per flyer type. The dotted pattern represents the blank, the square pattern represents the flyer with the university logo, and the diagonal line pattern represents the phishing flyer.

4.3 University Logo Survey Responses

Unfortunately, most users did not complete the survey. The only two responses were associated with the university logo flyer. Neither user reported having cybersecurity training and neither consider themselves to be experts. They were moderately and slightly concerned with cybersecurity. They were neutral about their planned future QR code scanning behavior. When prompted about their motivations for scanning the QR code, both of their responses centered around curiosity (e.g., why is the QR code blank?).

5. Discussion

In this study, we obtained a measure of QR code engagement on a large university campus in the southeastern region of the United States of America. Given the size of our campus student population, we discovered that engagement with our QR codes was low. While his level of engagement was similar to a previous on-campus study [20], the total number of engagements (22 users) was unexpectedly low. Because engagement was indexed only by participants who followed the QR code link, it is possible that other methods of engagement were missed. For instance, overall engagement rates might be higher if engagement included QR code use along with the total number of views of the flyers themselves. Without knowing precise viewing rates, it is difficult to gauge the exact impact of each flyer design. Even so, we find it unlikely that the flyers went unviewed. High-traffic locations and sustained visibility were key aspects of this procedure. Specifically, the flyers were placed in high-traffic campus areas, like the library and student center, for a week. Second, a research assistant ensured the flyers' visibility every two or three days.

Another consideration tied to engagement is viewer motivation. Due to the naturalistic aspects of the study, it was not possible to know in advance the proportion of individuals who would encounter each QR code design or predict their individual motivations. For instance, it is possible that more engagement with the phishing flyer was observed because a high proportion of participants also happened to be looking for a job. Similar types of motivated searching are less likely to drive interactions with the other two QR code flyer designs.

Using the QR code out of curiosity, as reported by these two participants, supports the findings of other QR code studies [4, 20]. Similarly, curiosity and alignment with the situational context (i.e., needing a job) are reported reasons for falling victim to phishing scams [22, 23].

Even with the overt report that they used the QR code out of curiosity, data from two participants must be considered with caution. The majority of the data collected suggest that informational cues were related to QR code engagement. Specifically, as we predicted, as informational cues increased, engagement with the flyers increased. The most scanned flyer was the phishing fake job ad, followed by the university logo and the blank flyer. Greater engagement with the university logo QR code compared to the non-branded QR code replicates previous findings [19] that QR code users are more likely to trust flyers with band logos. The fact that the phishing fake job ad had

more engagement than the simple branded logo, suggests that providing relevant content as an informational cue can further increase trust. While these results are not consistent with Vidas et al. (2013) (i.e., QR code-only flyers had the most engagement), we believe this difference reflects users' growing awareness of threats associated with QR coding usage [19]. Although QR code use presents personal and, potentially, professional risk, we are encouraged to see low engagement with suspect QR codes. This technology, like others, has advanced to a point that it is easy to use and has wide-ranging appeal. As usage has increased, agents who create malicious QR codes have become more skillful at disguising QRishing attacks making it difficult for users to determine risk. Because of this, users may have to become overly dependent on QR code reader security features.

References

1. Cain, A. A., Edwards, M. E., & Still, J. D.: An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications, 42, 36–45 (2018).
2. Morris, T.W., & Still, J.D.: Cybersecurity hygiene: Blending home and work computing. In W. Patterson (Ed.), New Perspectives in Behavioral Cybersecurity. Boca Raton, FL: CRC Press (2023).
3. Gabe, L.: What was that? Coinbase's QR code Super Bowl commercial confuses viewers.. https://www.usatoday.com/story/sports/Ad-Meter/2022/02/13/coinbase-qr-code-super-bowl-ad-crypto-commercial-confuses-viewers/6778949001/ (2022).
4. Seeburger. J.: No cure for curiosity: linking physical and digital urban layers. In Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design, pages 247–256. ACM (2012).
5. Vidas, T. Owusu, E. Wang, S. Zeng, C.. Cranor, L. F &. Christin, N. QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. In Proceedings of the 2013 Workshop on Usable Security (USEC'13) (2013).
6. Ozkaya, E., Ozkaya, H. E., Roxas, J., Bryant, F., & Whitson, D.: Factors affecting consumer usage of QR codes. Journal of Direct, Data and Digital Marketing Practice, 16, 209–224 (2015).
7. Dreyer, K.: 20 million Americans scanned a QR Code in October. Retrieved from https://www.comscore.com/Insights/Infographics/20-Million-Americans-Scanned-a-QR-Code-in-October, assessed Jan. 18, 2024.
8. Ricson, E.: QR code usage statistics 2022-2023: 433% scan increase and 438% generation boost. Retrieved from https://www.qrcode-tiger.com/qr-code-statistics-2022-q1, assessed Jan. 18, 2024.
9. Sharevski, F., Devine, A., Pieroni, E., & Jachim, P.: Phishing with malicious QR codes. 2022 European Symposium on Usable Security (2022).
10. Mitnick, K. D., & Simon, W. L.: The art of deception: Controlling the human element of security. John Wiley & Sons (2003).
11. Yeboah-Boateng, E. O., & Amanor, P. M.: Phishing, SMiShing & Vishing: an assessment of threats against mobile devices. Journal of Emerging Trends in Computing and Information Sciences, 5, 297-307 (2014).

12. Dhamija, R., Tygar, J.D., & Hearst, M.: Why phishing works. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI), ACM Press, Montreal, Canada (2006).
13. Krombholz, K., Peter, F., Peter, K., Ioannis, K., Markus, H., & Edgar, W.: 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 (2014).
14. Alsharnouby, M., Alaca, F., & Chiasson, S.: Why phishing still works: User strategies for combating phishing attacks. International Journal of Human-Computer Studies 82, 69–82 (2015).
15. Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F.: Human factors in phishing attacks: a systematic literature review. ACM Computing Surveys (CSUR), 54, 1-35 (2021).
16. Picard, J., Landry, P., & Bolay, M.: Counterfeit detection with QR codes. Proceedings of the 21st ACM Symposium on Document Engineering (2021).
17. Barr, L..: 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 (2022).
18. ReliaQuest: QR code phishing: 4 ways scanners are being scammed. Retrieved from https://www.reliaquest.com/blog/qr-code-phishing/ assessed Jan. 18th, 2024.
19. Kumar, N., Jain, S., Shukla, M., & Lodha, S.: Investigating Users' Perception, Security Awareness and Cyber-Hygiene Behaviour Concerning QR Code as an Attack Vector. In: Stephanidis, C., Antona, M., Ntoa, S. (eds) HCI International 2022 Posters. HCII 2022. Communications in Computer and Information Science, vol 1583. Springer, Cham (2022).
20. Vidas, T., Owusu, E., Wang, S., Zeng, C.,. Cranor, L. F, &. Christin, N. QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. In Proceedings of the 2013 Workshop on Usable Security (USEC'13) (2013).
21. Old Dominion University: Safe Computing. Retrieved from https://www.odu.edu/information-technology-services/security/safe-computing on 1/18/24.
22. Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R.: Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51, 576-586 (2011).
23. Moody, G. D., Galletta, D. F., & Dunn, B. K.: Which phish get caught? An exploratory study of individuals′ susceptibility to phishing. European Journal of Information Systems, 26, 564-584 (2017).