

Like Phishing in a Pond: Preliminary Results of a Realistic Hybrid QRishing Simulation Campaign in a Large Business Organization

Mattia Mossano
Karlsruhe Institute of Technology

Jennifer Vander Loop
DePaul University

Filipo Sharevski
DePaul University

Abstract

QR code phishing, or *QRishing*, is a neglected, yet very effective phishing threat. Individuals neither suspect QR codes nor smartphone QR code scanners offer usable security interventions against it. Business communication increasingly turns to QR codes due to their convenience, though whether employees are prepared to deal with this shift is hardly known. We address this gap by conducting a *realistic, hybrid QRishing simulation campaign* within a large business organization in the US, employing both digital and physical QRishing pretexts. Our preliminary results show a 12.4% QR code scan-through rate for the digital pretext, and an encouragingly low 0.5% scan-through rate for the combined physical pretexts.

1 Introduction

Phishing through QR codes, or *QRishing* [12], is on the rise: Microsoft reported a 146% increase in emails containing phishing QR codes in the first quarter of 2026 [5], and Palo Alto found that at least 15% of all web pages contains phishing QR codes [7]. Current awareness interventions hardly prepare individuals beyond emails [6], with public advisories (e.g., FTC [3]) being only vaguely informative. In the business sector, preliminary evidence shows that QRishing through emails reached a 30% scan-through rate [13]. Yet, QRishing also happens in the physical word, not only through emails [9].

The *goal* of our research is to address precisely this gap. We conducted a hybrid QRishing campaign within a large company in the US employing four distinct pretexts (one digital and three physical), each associated with a “phishing” QR

code (see Section 2.2). Once accessed, the URLs encoded in the QR codes redirected employees to the same survey, inviting them to a 10-minutes follow-up interview. In total, 51 employees completed the survey, and seven employees participated in the follow-up interviews (more details in Section 3).

The results revealed that the scan-through rates of the email pretext were lower than other QRishing evaluations, but on-par with traditional email evaluations [10]. However, the scan-through rates of the physical pretexts were reassuringly low, largely thanks to *word of mouth* among employees, despite the considerable foot traffic present on the company premises.

2 Methodology

2.1 Research Questions

The study addressed two exploratory research questions:

RQ1. How prone are employees that scan QR codes included in physical pretexts to scan-through to the landing webpage encoded in a QR code?

RQ2. How prone are employees that scan QR codes included in digital pretexts to scan-through to the landing webpage encoded in a QR code?

2.2 Attack Vectors and Infrastructure

To answer our research questions, we designed a realistic, hybrid QRishing campaign employing both physical and digital pretexts: 1) an *email*, 2) a *standalone QR code*, 3) a *physical flyer*, and 4) a *digital billboard*. Each pretext included a QR code encoding a URL with one of three URL deception techniques (described in [11]): *Mangle* for the email URL, *Random Characters* for the standalone QR code and the digital billboard, and *Subdomain* for the physical flyer. Each of the hooks, be it the email sender name and address, the corporate layouts, or the references to in-house associations, was obtained by one of the researchers through an *Open Source Intelligence* investigation to simulate the knowledge available to an attacker without insider help. Each URL was

under the control of the collaborating large business (*hereafter*, the company), which bought them specifically for the hybrid QRishing campaign to avoid exposing their employees to unnecessary risks. A table with the specific URLs is in Appendix B, followed by images of how the pretexts looked during the campaign in Appendix C.

2.3 Data Collection

The email pretext was disseminated by the company’s IT department to 1529 employees. The standalone QR code, physical flyer, and digital billboard were placed by a team of two researchers on the premises of one of the company’s buildings, to which they were granted access for the duration of the campaign. As such, even if the pretexts were believable attackers’ products (as mentioned in Section 2.2), no actual attack took place, and the company was informed and approved every aspect of the campaign. The email campaign was executed at 11:37 AM on Tuesday, November 11, 2025, while the remaining vectors were shown from 11:00 AM to 4:00 PM on both Tuesday, November 11, 2025, and Wednesday, November 12, 2025. The dates were chosen to align with the days of highest employee presence in the selected building, with 582 and 467 employees, respectively, visiting.

3 Results

3.1 Quantitative Results

According to the metrics collected by the company, 52.2% of the target employees actually opened and read the email, out of which 54.5% reported the email as suspicious. A total of 45 employees scanned the QR, resulting in a 3% targeted scan-through rate. Considering only those employees who opened the email, the campaign resulted in a 5.6% scan-through rate. Of those employees who didn’t report the email, the campaign resulted in a 12.4% effective scan-through rate.

Only five employees scanned the physical flyer or the standalone QR code, though more may have abandoned the survey at the start. Only one employee scanned the digital billboard. Considering the number of employees who accessed the buildings on the campaign days, the physical component of the campaign resulted in a 0.5% scan-through rate.

3.2 Interview Results

Seven of the 51 employees who scanned the QR code in any capacity agreed to be interviewed, i.e., a 13.7% turnout rate (see the interview script in Appendix A). Six of them scanned it through the email, and one scanned the standalone QR code. The qualitative interviews revealed four distinct themes leading to scanning:

- i) *Campaign Sophistication*. All the interviewees agreed that this was the most sophisticated campaign to take

place at the company, especially because they based their judgment on the email sender (which was “spoofed”) and the corporate layout used.

- ii) *Authority Effect*. For the email, the use of the CSO’s company email address increased the legitimacy of the email, which was related to enabling two-factor authentication.
- iii) *Missing URL Inspection*. All the interviewees did not inspect the URLs before visiting them, effectively making it impossible for them to notice the “attacks”.
- iv) *Word of mouth*. The employee that fell for the physical pretext warned their colleagues that the company was “out to suss [them]... as with those test emails they sometimes send”.

4 Discussion & Conclusion

The 12.4% scan-through rate reached in the email pretext is considerably lower than the 53% scan-through rate reported in Kowalewski et al. [4] for general individuals. Yet, if we compare the scan-through rate to the 16.22% click-through rate of phishing emails [1], we can see that the difference is considerably lower. This might indicate that, even if employees pay more attention at work, they are just as susceptible to QRishing attacks as they are to phishing emails.

However, because awareness interventions heavily focus on emails [6], it is possible that the increase in QRishing attacks will see a corresponding increase of risk that is left unaddressed. This lack of coverage is also surprising, given that employees generally react positively to how to spot a phish beyond just emails [8]. Another reason for our finding is that the pretexts might have influenced the way the employees approached the email – from an email about 2FA setup (sent by an *authoritative* figure), to a community group participation within the organization (appealing to *liking* and *belonging* per the updated Cialdini’s principles of influence [2]).

That our interviews highlighted the reliance on *word of mouth* could also be a symptom of a need for support waiting to be addressed. This reliance might also explain the considerably lower scan-through rate for the physical pretexts, which novelty might have increased the exchange among peers due to not being “yet another phishing email.” Admittedly, another reason for the physical pretexts’ lower scan-through rates might simply be that employees are focused on their tasks, ignoring QR codes around the office and common spaces.

As a future work we already extended the organization’s phishing awareness training to cover QRishing as well, incorporating the extensive interviews’ feedback about the employees’ perceptions, reaction, and reasoning around the tested QR codes. The next step is to evaluate the awareness intervention we disseminated it among their employees by replicating the hybrid QRishing campaign in a different location, new set of employees, and QR code embeddings with both phishing and legitimate URLs.

References

- [1] Eric B Blancaflor, Adrian B Alfonso, Kevin Nicholas U Banganay, Dela Cruz, Karen E Fernandez, and Shawn Austin M Santos. Let's Go Phishing: A Phishing Awareness Campaign Using Smishing, Email Phishing, and Social Media Phishing Tools. In *International Conference on Industrial Engineering and Operations Management*, IEOM '11, Singapore, SG, 2021. <https://ieom.society.org/singapore2021/papers/1105.pdf>.
- [2] Robert Cialdini. The Science of Persuasion Seven Principles of Persuasion, 2022. <https://www.influenciateatwork.com/7-principles-of-persuasion/>.
- [3] Federal Trade Commission. Scammers hide harmful links in QR codes to steal your information, 2023. <https://consumer.ftc.gov/consumer-alerts/2023/12/scammers-hide-harmful-links-qr-codes-steal-your-information>.
- [4] Marvin Kowalewski, Leona Lassak, Markus Dürmuth, and Theodor Schnitzler. Scanned and Scammed: Insecurity by ObsQRity? Measuring User Susceptibility and Awareness of QR Code-Based Attacks. In *USENIX Security Symposium*, USENIX Security '25, pages 1415–1434, Seattle, WA, US, 2025. USENIX. <https://dl.acm.org/doi/10.5555/3766078.3766152>.
- [5] Microsoft Threat Intelligence and Defender Security Research Teams. Email threat landscape: Q1 2026 trends and insights, 2026. <https://www.microsoft.com/en-us/security/blog/2026/04/30/email-threat-landscape-q1-2026-trends-and-insights>.
- [6] Mattia Mossano, Kami Vaniea, Lukas Aldag, Reyhan Düzgün, Peter Mayer, and Melanie Volkamer. Analysis of Publicly Available Anti-phishing Webpages: Contradicting Information, Lack of Concrete Advice and Very Narrow Attack Vector. In *2020 IEEE EuroS&P Workshops (EuroS&PW)*, pages 130–139, Online, 2020. IEEE. <https://ieeexplore.ieee.org/document/9229741>.
- [7] Palo Alto. Phishing on the edge of the web and mobile using qr codes, 2026. <https://unit42.paloaltonetworks.com/qr-codes-as-attack-vector/>.
- [8] Katharina Schiller, Florian Adamsky, Christian Eichenmüller, Matthias Reimert, and Zinaida Benenson. Employees' attitudes towards phishing simulations: "it's like when a child reaches onto the hot hob". In *Proceedings of the 2024 on ACM CCS*, ACM CCS '24, page 4167–4181, New York, NY, USA, 2024. Association for Computing Machinery. <https://doi.org/10.1145/3658644.3690212>.
- [9] Filippo Sharevski, Mattia Mossano, Maxime Veit, Gunther Schiefer, and Melanie Volkamer. Exploring Phishing Threats through QR Codes in Naturalistic Settings. In *Symposium on Usable Security*, USEC 2024, page 17, Reston, VA, US, 2024. Internet Society. <https://www.ndss-symposium.org/wp-content/uploads/usec2024-50-paper.pdf>.
- [10] Jan Tolsdorf, David Langer, and Luigi Lo Iacono. Phishing susceptibility and the (in-)effectiveness of common anti-phishing interventions in a large university hospital. In *Proceedings of the 2025 ACM CCS*, CCS '25, page 4334–4348, New York, NY, USA, 2025. Association for Computing Machinery. <https://doi.org/10.1145/3719027.3765164>.
- [11] Maxime Veit, Mattia Mossano, Tobias Länge, and Melanie Volkamer. Comprehensive List of User Deception Techniques in Emails, 2026. <https://doi.org/10.48550/arXiv.2604.04926>.
- [12] Timothy Vidas, Emmanuel Owusu, Shuai Wang, Cheng Zeng, Lorrie Faith Cranor, and Nicolas Christin. QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. In *Financial Cryptography and Data Security 2013*, FC '13, pages 52–69. Springer, 2013. https://doi.org/10.1007/978-3-642-41320-9_4.
- [13] Marie Weinz, Nicola Zannone, Luca Allodi, and Giovanni Apruzzese. The impact of emerging phishing threats: Assessing quishing and LLM-generated phishing emails against organizations. In *Proceedings of the 20th ACM AsiaCCS*, ASIA CCS '25, page 1550–1566, New York, NY, USA, 2025. Association for Computing Machinery. <https://doi.org/10.1145/3708821.3736195>.

A Interview Questions

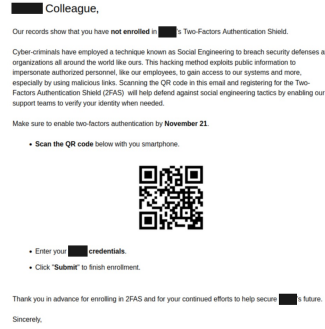
1. How did you encounter the QR code we used as part of the internal phishing test?
2. Did you made any assessment before scanning the QR code?
3. Once you assessed the QR code and the communication (e.g., the email, the physical QR codes, the digital billboard), how did you decide to proceed?
4. Did you at any point scan the QR code (e.g., in the email, on the physical QR codes, on the digital billboard) and abandon tapping the link?
5. Do you usually scan QR codes?
6. When you scanned the QR code in our test phishing campaign, did you inspect the domain URL in the displayed frame of the scanner (e.g., read the link name of the website embedded in the QR code)?

B URLs Used in the Hybrid QRishing Campaign

Pretext	Obfuscation Techniques	URL
Email	Mangle	https://2ebra.net
Standalone QR Code	Random Characters	https://host350.org
Physical Flyer	Subdomain	https://zebra.com.unidoz.info
Digital Board	Random Characters	https://host350.org

Table 1: URLs used in the study and the URL obfuscation techniques used. The URL obfuscation techniques are based on [11].

C Pretexts and Examples of their Placements



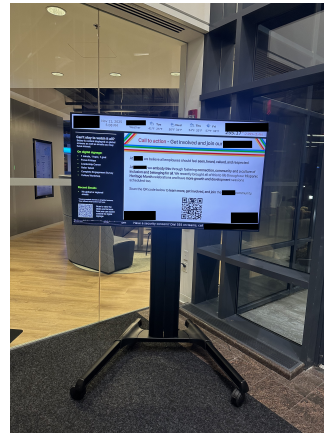
(a) Email pretext



(b) Standalone QR code pretext



(c) Physical flyer pretext



(d) Digital billboard pretext

Figure 1: Pretexts used in the hybrid QRishing campaign, and examples of their placements.