From Scanning to Action: An Observational Study of User Decision-Making in QR-Code Emails

Shojiro Takahara
Waseda University

Rei Yamagishi
Waseda University

Ryo Iijima
AIST, Waseda University

Tatsuya Mori
Waseda University, NICT, RIKEN AIP

1 Introduction

Quishing has emerged as a major phishing variant: QR-code-bearing emails rose from 0.8% to 10.8% of all phishing attacks between 2021 and 2024 [1]. Three structural properties distinguish quishing from URL-based phishing. First, the destination URL is hidden until the QR code is scanned, so URL-based heuristics taught in security training cannot inform the user's decision before they act. Second, scanning is a cross-device smartphone action that has become a deeply habitual everyday behavior, often performed with low vigilance. Third, because QR codes are embedded as images, they can evade traditional URL filtering and text-based email analysis, making automated detection more difficult.

This study aims to identify human-centered challenges and requirements for quishing mitigation by analyzing users' behaviors and thought processes when they encounter quishing emails. We address three questions:

RQ1. What processes and thoughts do users go through when viewing quishing emails?

RQ2. How do differences in the perception of URLs versus QR codes influence the decision to scan?

RQ3. What inherent difficulties arise in implementing countermeasures against quishing?

We make three contributions. First, we extend Wash et al.'s phishing decision-making model [2] with QR-code-specific factors at each process, as shown in Figure 1, revealing a post-scan verification step that almost all users omit. While prior work has quantified quishing susceptibility in email tasks [3] and naturalistic physical settings [4], the underlying decision process has not been characterized. Second, we derive design requirements for scanning applications, namely mandatory cool-down periods combined with explicit visualization of destination safety. Third, we show that quishing awareness lags markedly behind general phishing awareness even among prepared users, motivating dedicated security education, an incident-sharing system, and email-client design guidelines.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

2 Method

Overview. We conducted an observational study in which participants responded to simulated emails while thinking aloud, followed by an approximately 39-minute semi-structured interview. We qualitatively compared user reasoning across QR-code, URL, and button-based delivery; click/scan rates are reported only as descriptive context, not statistical inferences. Using a deception design, we withheld the phishing/quishing focus until post-task debriefing, after which participants reaffirmed consent. Each participant completed a pre-survey, briefing, practice email, eight-email think-aloud task, and interview (Figure 2 in the appendix). The design was refined through two pilot studies.

Participants. We recruited 20 participants through an online bulletin board at our institution using convenience sampling (16 students, 4 employed; aged 18–28), all daily PC and smartphone users (Table 1 in the appendix). Because our participant group was limited in size, our findings should be interpreted as qualitative observations within this population.

Task environment. To preserve safety without handling real credentials, we built a mock Japanese Gmail-style client on a study PC; QR codes were scanned with participants' own smartphones to preserve everyday device configurations.

Email dataset. Each participant viewed 8 emails selected from 14 stimuli across URLs, buttons, and QR codes (Table 2 in the appendix). Sets 7 (quishing) and 8 (phishing) were shown to all participants, ensuring that everyone encountered both a quishing and a phishing email; together with Set 1 (always QR-based), every participant saw at least two QR-code emails. Following Jayatilaka et al. [5], varying combinations

separate participant-level from email-level variance. Phishing materials (emails and URLs) were based on reported cases in Japan [6, 7].

Analysis. We analyzed transcripts from the observation tasks and interviews using thematic analysis [8]. Two coders independently performed inductive open coding, discussed discrepancies, and developed the codebook over five consensus meetings [9], yielding a hierarchical codebook of 278 codes. At most one new code emerged from the final participant, suggesting theoretical saturation [10].

Ethics statement. This study followed the Menlo Report [11] and was approved by our IRB. As deception was necessary to reflect real-world behavior, participants provided informed consent, were debriefed after the main task, and reaffirmed consent for data use; full compensation was guaranteed regardless of withdrawal. Data were anonymized, encrypted, and processed locally; compensation exceeded the local minimum wage.

3 Results

The three findings below motivate the extension (Figure 1); all counts describe observed patterns in N=20.

F1. Awareness gap at *Expecting* (RQ2) *Most* participants (N=14) reported never having considered QR codes as an attack vector: "I had never thought QR codes could be used for phishing." Without this prior expectation, quishing-specific suspicion did not form at the *Expecting* process, even among participants who were familiar with conventional phishing. By contrast, a few participants (N=3) had encountered public quishing reports and exhibited visibly higher vigilance.

F2. Non-deliberate scanning bypasses *Suspecting* through *Deciding* (RQ2) *Most* participants (N=15) described QR scanning as a routinized, curiosity-driven action. QR codes were perceived differently from visible URLs: their visual salience, novelty, and everyday familiarity encouraged participants to scan before forming suspicion. P10 explained: "When a QR code is sent, I feel more curious and want to scan it. I just think I'll scan it for now. I think my daily habits are influencing this." In our data, this scan-first impulse repeatedly overrode the Suspecting and Deciding processes that the original model places before Acting. We frame this as an observed behavioral pattern, not as a cognitive-capability claim.

F3. *Post-scan Investigating* and *Post-scan Deciding* are omitted (RQ3) Of the participants who scanned, *almost all* (N=18) did not investigate the destination URL after scanning, even when the scanning app displayed it. Only a *few* (N=2) re-executed any *Post-scan Investigating* step. Participants treated the post-scan URL as redundant rather than as new evidence: "I knew it was there, but my eyes just don't go there" (P13). Others reported that they would not be able to judge URL legitimacy even if they looked. Pre-scan trust judgments anchored post-scan evaluation, suggesting that URL display alone may be insufficient without interface support for *Post-scan Investigating* and *Post-scan Deciding*.

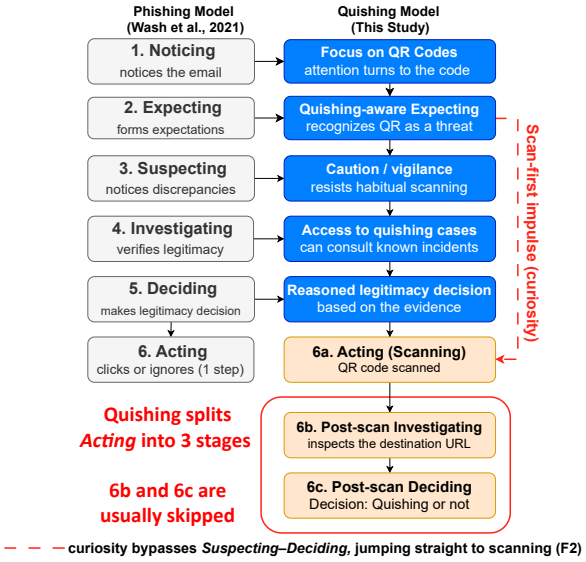

Figure 1: Proposed decision-making model for quishing emails, extending Wash et al.'s [2] phishing model. (RQ1)

4 Discussion

Quishing-specific risk factors. Quishing introduces three risks beyond URL-based phishing. First, QR codes visually attract attention and can be misread as legitimate rather than suspicious. Second, by shifting URL inspection from pre-action to post-scan, QR codes split decision-making into two stages: whether to scan and whether to open the displayed URL. However, the latter step is often skipped. Third, low quishing awareness prevents suspicion formation at *Expecting*, even among users cautious about general phishing.

Recommendations. These findings suggest three intervention points. First, QR-scanning applications should provide easy-to-understand destination-safety indicators backed by phishing-database lookups, not only raw URL strings, and may enforce a brief cool-down before tap-through, consistent with Caraban et al.'s *throttling* [12]. Second, email clients should detect in-body QR codes and warn users before scanning begins. Third, education and public advisories should treat quishing as a distinct category and support case-sharing to strengthen the *Expecting* process.

Limitations. Our N=20 participant group consisted mostly of Japanese university students, and the controlled mock-client environment may limit ecological validity. Future work should quantitatively validate the proposed model with larger, more diverse participant groups and more naturalistic environments.

References

[1] Egress Software Technologies. Phishing threat trends report 2024. Technical report, Egress Software Technologies Ltd., 2024. https://www.egress.com/.

[2] Rick Wash, Norbert Nthala, and Emilee Rader. Knowledge and capabilities that non-expert users bring to phishing detection. In *Proceedings of Seventeenth Symposium on Usable Privacy and Security (SOUPS'21)*, pages 377–396, 2021.

[3] 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 *Proceedings of the 34th USENIX Security Symposium (USENIX Security '25)*, pages 1415–1434, Seattle, WA, 2025. USENIX Association.

[4] Filipo Sharevski, Mattia Mossano, Maxime Veit, Gunther Schiefer, and Melanie Volkamer. Exploring phishing threats through QR codes in naturalistic settings. In *Proceedings of Symposium on Usable Security and Privacy 2024 (USEC'24)*, 2024.

[5] Asangi Jayatilaka, Nalin Asanka Gamagedara Arachchilage, and Muhammad Ali Babar. Why people still fall for phishing emails: An empirical investigation into how users make email response decisions. In *Proceedings of Symposium on Usable Security and Privacy 2024 (USEC'24)*, February 2024.

[6] Council of Anti-Phishing Japan. Phishing report and database, 2026. https://www.antiphishing.jp/ (Accessed: 2026-01-15).

[7] JPCERT/CC. phishurl-list: Phishing url list, 2026. https://github.com/JPCERTCC/phishurl-list/ (Accessed: 2026-01-15).

[8] Virginia Braun and Victoria Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[9] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for CSCW and HCI practice. In *Proceedings of the ACM on Human-Computer Interaction (CSCW)*, page Article 72, 2019.

[10] Greg Guest, Arwen Bunce, and Laura Johnson. How many interviews are enough?: An experiment with data saturation and variability. *Field Methods*, 18(1):59–82, 2006.

[11] David Dittrich and Erin Kenneally. The Menlo Report: Ethical principles guiding information and communication technology research. Technical report, U.S. Department of Homeland Security, August 2012.

[12] Ana Caraban, Evangelos Karapanos, Daniel Gonçalves, and Pedro Campos. 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI'19)*, pages 1–15. ACM, 2019.

A Appendix

A.1 Participant Demographics and Email Conditions

Table 1 reports participant demographics (age, status, security expertise, primary QR-scanning app, and interview duration), together with the email condition (A or B) assigned to each participant in Sets 1–6. The role, vector, and content corresponding to each condition are listed in Table 2.

A.2 Email Dataset and Click/Scan Rates

Table 2 lists the email materials used in the study together with per-email click/scan rates as descriptive context. For Sets 1–6, one of the two conditions (A or B) was randomly presented to each participant; Sets 7–8 were presented to all. "Click/Scan" indicates the percentage who clicked a URL/button or scanned a QR code.

A.3 Overview of the Study Procedure and Interview Structure

Figure 2 provides an overview of the study procedure and the semi-structured interview structure summarized in Section 2, including the pre-survey, briefing, practice trial, eight-email concurrent think-aloud task, and post-task debriefing followed by the semi-structured interview.

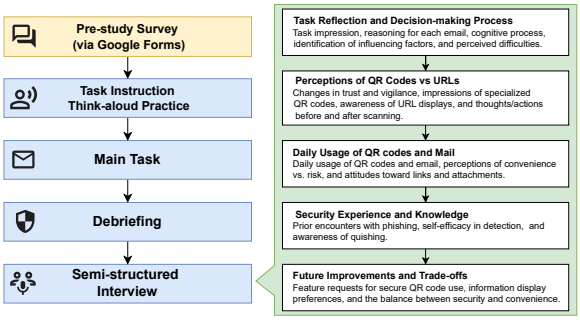

Figure 2: Overview of the study procedure and interview structure.

Table 1: Participant Demographics and Email Condition Assignment.

ID	Interview [min]	Age	Status	Security Expertise	Primary Scanning App	Email Condition Assignment					
						Set1	Set2	Set3	Set4	Set5	Set6
P01	36	20–22	Student	None	Android Cam.	A	B	A	A	B	A
P02	36	18–19	Student	Self-taught	iOS Cam.	B	A	B	A	A	B
P03	32	23–25	Student	None	iOS Cam.	A	B	B	B	A	B
P04	32	20–22	Student	None	iOS Cam.	B	A	A	B	B	A
P05	46	18–19	Student	None	Dedicated App	A	A	A	B	A	A
P06	51	23–25	Student	CS major	iOS Cam.	B	B	A	A	B	A
P07	34	23–25	Student	Self-taught	iOS Cam.	A	A	A	A	B	B
P08	32	20–22	Student	Self-taught	Android Cam.	B	B	B	B	A	B
P09	35	20–22	Student	Self-taught	iOS Cam.	B	A	A	A	B	A
P10	47	18–19	Student	Self-taught	Google Lens	A	B	B	B	A	B
P11	33	26–28	Student	Self-taught	Android Cam.	A	B	B	A	B	B
P12	44	20–22	Student	None	Android Cam.	B	A	A	A	A	B
P13	37	23–25	Student	Self-taught	Android Cam.	A	B	B	A	B	A
P14	36	20–22	Student	None	iOS Cam.	B	A	A	B	A	A
P15	31	20–22	Student	Self-taught	iOS QR Scanner	B	A	B	B	B	B
P16	40	18–19	Student	None	iOS Cam.	A	B	B	B	A	A
P17	36	23–25	Employed	Self-taught	Android Cam.	B	B	A	A	B	B
P18	52	23–25	Employed	None	iOS Cam.	A	B	B	B	A	A
P19	36	23–25	Employed	Self-taught	iOS Cam.	A	A	A	B	B	B
P20	47	26–28	Employed	Self-taught	iOS Cam.	B	A	B	A	A	A

Note: Interview [min]: duration of the semi-structured interview. Set1–Set6 show which condition (A or B) was assigned to each participant in Sets 1–6; the role, vector, and content of each condition are listed in Table 2. Security Expertise: None = no formal or informal training; Self-taught = independently learned; CS major = computer science or related field.

Table 2: Email Dataset Configuration and Click/Scan Rates.

Set	Role	Vector	Content	Click/Scan (%)
1-A	Legitimate	QR	Unrecognized sign-in alert	50
1-B	Quishing	QR	Request for 2FA setup	50
2-A	Legitimate	URL	Reward for meeting conditions	40
2-B	Phishing	URL	Reward for meeting conditions	30
3-A	Legitimate	URL	Credit card payment error/confirmation	70
3-B	Phishing	URL	Credit card payment error/confirmation	40
4-A	Legitimate	Button	Request for 2FA setup	50
4-B	Phishing	Button	Request for 2FA setup	80
5-A	Legitimate	QR	Login from a different device	20
5-B	Legitimate	URL	Login from a different device	40
6-A	Quishing	QR	Reward for meeting conditions	50
6-B	Phishing	URL	Reward for meeting conditions	70
7	Quishing	QR (Logo)	Account re-authentication	65
8	Phishing	URL	Account re-authentication	50

Note: For Sets 1–6, one of the two conditions (A or B) was randomly presented to each participant; Sets 7 and 8 were presented to all participants. "Click/Scan" indicates the percentage of participants who clicked a URL/button or scanned a QR code for the corresponding email.