USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

Scanned and Scammed: Insecurity by ObsQRity? Measuring User Susceptibility and Awareness of QR Code-Based Attacks

Marvin Kowalewski and Leona Lassak, *Ruhr University Bochum;*
Markus Dürmuth, *Leibniz University Hannover;*
Theodor Schnitzler, *Maastricht University*

https://www.usenix.org/conference/usenixsecurity25/presentation/kowalewski

This paper is included in the Proceedings of the
34th USENIX Security Symposium.

August 13–15, 2025 • Seattle, WA, USA

978-1-939133-52-6

Open access to the Proceedings of the
34th USENIX Security Symposium is sponsored by USENIX.

Scanned and Scammed: Insecurity by ObsQRity? Measuring User Susceptibility and Awareness of QR Code-Based Attacks

Marvin Kowalewski[*], Leona Lassak[*], Markus Dürmuth[†], Theodor Schnitzler[◇]
[*]*Ruhr University Bochum,* [†]*Leibniz University Hannover,* [◇]*Maastricht University*

Abstract

QR codes offer a seamless user experience and have become universal – from accessing websites over handling payments to using electric vehicles. However, their nature of displaying embedded data in a non human-readable format raises concerns about their misuse. While traditional phishing and scams are well-studied, how QR codes might increase users' exposure to such threats remains under-explored. Our research explores users' susceptibility to QR code-based scams and phishing and examines their perception of, experiences with, and (mis)understandings about QR codes. Across three experiments with 1,876 participants, we simulated everyday tasks like online payments and shopping, comparing user reactions to traditional and QR code-mediated attacks. While several participants detected traditional phishing, almost no one identified QR-based attacks. Similarly, only 13 % recognized fraudulent QR payment requests, compared to 46 % with manually entered payment details. These findings highlight the need for security measures, as users tend to be unaware of QR codes' characteristics and potential for misuse.

1 Introduction

QR codes have become an integral part of today's life, offering seamless interactions for various purposes, such as redeeming tickets and vouchers, downloading apps, and enabling quick and easy online logins and payments [5, 24, 57, 63]. They are often deployed as a fast, frictionless alternative to manual inputs and traditional interfaces to simplify everyday interactions [57, 63]. Beyond their usability benefits, QR codes are remarkably easy to generate, highly scalable, and cost-effective, further contributing to their widespread adoption across diverse industries and use cases [9, 44]. However, this low barrier also makes them an interesting target for misuse. In the physical world, attackers have already exploited QR codes. By placing malicious overlays on legitimate ones in public locations such as parking meters or electric vehicle charging stations they phish user data, deceive users into downloading malicious apps, or even transferring money to an attacker's account [15, 49].

Similarly, large-scale digital scams have leveraged QR codes in phishing campaigns, disguising malicious links in emails pretending to be from trusted organizations. These QR codes obscure the destination domain, leading unsuspecting users to phishing websites or prompting them to transfer money directly to scammers (e. g., pretending to be a charity organization) [4, 20, 29, 33]. Institutions, particularly banks, have started issuing warnings to educate users about these risks [19, 25, 53, 54]. Early studies also demonstrated users' limited awareness of the potential risks associated with QR codes, for example, luring users into scanning QR codes in public places using emotional appeals [3, 59, 60]. Other research showed that curiosity and convenience drive users to scan QR codes without carefully scrutinizing the associated URLs [58, 67]. Unlike traditional hyperlinks, QR codes are machine-readable by design and obscure their content to the human eye. Without technical tools, it is impossible to assess their content or destination. This curiosity-based, "careless" scanning, combined with low awareness of associated risks, and the inability to determine legitimacy without interaction, makes QR codes particularly attractive for malicious actors.

While traditional online phishing and fraud have been extensively studied, the unique risks of QR codes online remain under-explored. We fill this gap by investigating whether users verify the data concealed by QR codes or whether they blindly accept them as authentic. We also explore users' understanding and comprehension of (malicious) QR codes. Specifically, we answer the following research questions:

- **RQ 1** How do QR codes influence users' susceptibility to common online attack vectors like payment scams or phishing?
- **RQ 2** What strategies do users' have to determine the legitimacy of QR codes?
- **RQ 3** What real-life experiences do users have with malicious QR codes and what beliefs and misconceptions do they hold about QR code misuse?

To answer these questions, we conducted two independent online studies in Germany, with 858 and 888 participants, respectively. In both studies, participants completed a simulated scenario, inspired by common, real-world activities: *online shopping* and *online payments*. Our main goal was to *measure* how using QR codes in typical online attack vectors like phishing and scam affects participants' susceptibility compared to traditional methods using just links or text.

(I) In the *Shopping* scenario, participants interacted with an online shopping website and received typical emails, such as order confirmations or coupons. Depending on their assigned condition, these emails included either legitimate content or simulated phishing attempts.

(II) In the *Payment* scenario, participants performed a transaction using an online banking app. In this case, the transaction details were either legitimate or malicious.

In short, both studies used a 2x2 between-subjects design with two independent variables: the *Legitimacy* (legitimate vs. malicious) of the request, and the *Interaction Method* (traditional vs. QR code). For the Shopping scenario, we conducted an additional small-scale study ($n = 130$) exploring shortened URLs, given that they share the content-masking characteristic of QR codes by concealing the actual destination domain. Our work demonstrates that users struggle to distinguish malicious QR codes from legitimate ones, primarily due to a lack of knowledge of QR codes' characteristics and unawareness of their potential for misuse. From these results, we derive design recommendations for QR code applications such as introducing short delays when interacting with QR codes, and discuss proactive technical measures that may increase users' awareness, to ultimately help better protect users from modern QR code-based attacks.

2 Background and Related Work

The following sections provide a high-level introduction to common phishing practices, explain technical details of QR codes and short URLs, and outline related research on QR code-based phishing and scam attacks.

Phishing Attacks and Financial Scam Prevalent phishing attacks, typically delivered via email, seek to exploit users' trust by impersonating legitimate entities to steal sensitive information, such as login credentials or payment details [38]. Phishing emails usually evoke a sense of urgency (or scarcity), such as warnings about password changes or account deactivation, or offer financial incentives like discounts or prizes. In other cases, they appeal to users' emotions by soliciting donations for humanitarian aid related to natural disasters, wars, or pandemics [6, 21, 28, 32]. Commonly, attackers embed a hyperlink in these emails (often disguised as a button), which redirects the user to a phishing website. This fraudulent site typically mimics a legitimate one but leads to a different domain – i. e., using *cybersquatting* or *typosquatting* techniques, or adding additional subdomains to deceive users [50]. Users often struggle to identify these obfuscated look-alike attacker URLs [52]. Unfortunately, current browser highlighting techniques and URL formatting aids in email clients show little evidence of effectively assisting users [42]. Prior research indicates that once users are willing to click on a link in a phishing email, the majority also proceeds to submit their sensitive information, i. e., fall for the phishing attempt [38, 39], indicating an overreliance on the email's visual appearance as a trust signal [31, 47, 68].

QR Codes  Quick Response (QR) codes are two-dimensional matrix bar codes, developed in the 1990s, when traditional barcodes reached their data capacity limits in automotive manufacturing [12]. The array of square pixels encodes up to 7,089 numeric or 4,296 alphanumeric characters as machine-readable data. Three of the four corners contain a unique pattern, enabling reliable detection of position, size, and orientation for scanning from various angles The QR code standard supports a wide range of sizes and four levels of error correction [27]. By default, Reed–Solomon error correction[1] enables decoding if up to 30% of a QR code is damaged or visually obstructed (e.g., by logos) [11].

Wide Applications. Their versatility and ease of use made QR codes' popular in various applications (e. g., URL redirection, online payments, digital health certificates, event ticketing). Specialized formats like EMV QR codes [16] support secure financial transactions by enabling standardized communication between merchants and payment service providers. Secure QR Codes (SQR) for high-assurance contexts like digital identity, healthcare (e. g., COVID-19 certificates), and government services incorporate cryptographic signatures or encrypted payloads to ensure authenticity, prevent tampering, and protect sensitive information [17, 23].

Non Human-Readable. The visual appearance of QR codes provides no intuitive cues about their encoded content. Without scanning, this inherent obfuscation makes it difficult for users to assess the legitimacy or trustworthiness of the source or the data embedded within the code [3].

Short URLs Short URLs simplify sharing long and complex links, especially via social media, messaging platforms, or emails. A URL shortening service converts long URLs into a compact alias, typically using a random or user-chosen string, incremental ID, or a hash of the original URL (e.g., `tinyurl.com/usenix2025`). When users click on a short URL, the request is redirected to the shortening service, which

[1] Reed–Solomon codes robustly recover data at byte level by using twice the number of redundant codewords as the number of errors to be corrected.

looks up the alias in its database, retrieves the corresponding long URL, and seamlessly redirects to the intended destination [61]. Like QR codes, short URLs inherently obscure their actual destination which prevents easy inspection of the underlying content before accessing it, raising similar questions about transparency and security.

2.1 Studies on (Malicious) QR Codes

Krombholz et al. [35] were the first to investigate threats related to QR codes, i. e., attackers replacing entire QR codes. Their analysis of different use cases for QR codes (e. g., mobile payments, access control, and advertising) revealed several open research challenges, distinguishing between security awareness issues and challenges tied to usable security design guidelines. As a follow-up, Krombholz et al. [36] examined potential security vulnerabilities in deployed QR code scanner apps and proposed a set of design recommendations aimed at more effectively protecting users from being deceived by malicious QR codes. Vidas et al. [67] conducted a qualitative study exploring the viability of QR code-initiated phishing attacks. In two experiments, they captured peoples' interaction with contextless QR codes in public spaces such as bus stops, restaurants, or printed on flyers. 85% of those who scanned a QR code also proceeded to visit the associated website, stating *curiosity* as a primary motivator for scanning. Seeburger [58] confirmed these findings, highlighting curiosity as the main driver for scanning non-contextual QR codes.

Sharevski et al. [59] conducted an online study with 173 participants to investigate *quishing* – a form of phishing that leverages malicious QR codes – redirecting participants to a phishing website where they were prompted to log in using Google or Facebook single sign-on. 67% of participants were willing to use these login credentials. A subsequent study by Sharevski et al. [60], reinforced these findings with QR codes in public spaces, where the same number of participants (67%) accessed the website without inspecting the URL for phishing cues. Notably, 19% of participants explicitly cited limitations in the QR code scanner app interface as their reason for not examining the URLs.

QR codes are designed to function even if up to 30% of their content is missing or obstructed. This enables visual modifications, such as altering colors or embedding logos in the QR code. Bekavac et al. [3] leveraged these visual alterations as a security feature to help users detect manipulated QR codes in public spaces. In a 2x2 factorial design, they investigated users' ability to differentiate legitimate and manipulated versions with both *simple* (plain) and *visually* customized QR codes. By placing posters at Christmas markets advertising 50 € coupons, they showed that users were significantly less likely to scan the malicious *visual* QR codes than the plain ones as 71% were able to identify them as suspicious, in contrast to only 36% for the latter one.

3 Method

To study users' susceptibility to QR code-based attacks in a practical environment, we conducted two independent online experiments with 858 (Study I – Shopping) and 888 participants (Study II – Payment) in Germany between February and June 2024. To contextualize the findings from Study I, we conducted an additional small-scale experiment using short URLs with 130 participants in May 2025. In each experiment, participants completed a practical task representing one of two common *use cases* for QR codes. In Study I, participants ordered items from an online shop using a QR code-based coupon. In Study II, participants made an online payment using the QR code scanning feature of an online banking app. Both the app and the online shop website were specifically developed for the purpose of these studies. As the two studies represent distinct use cases of QR codes with different contextual applications and study designs, we do not compare participants' susceptibility across them. Instead, by covering two use cases, we aim to reflect a broader spectrum of applications, thereby enabling more generalizable insights into users' interaction with QR codes in everyday contexts.

High-level Study Design On a high level, the studies followed similar procedures, capturing QR codes' influence on participants' ability to detect phishing and scam attacks. Participants interacted with either a QR code or a "traditional" interaction method such as a link or manual typing. In Study I, the QR code encoded a URL, which participants scanned using any general-purpose QR scanner app (e.g., their phones' default camera app). The corresponding website was opened in the device's default web browser. In Study II, participants used a dedicated payment app resembling apps like Paypal, WeChat Pay, or AliPay. The app's internal QR code scanner automatically extracted payment details from dedicated payment QR codes to streamline the transaction process. We further detail these methods in the use case-specific sections. Participants were invited to join a study for testing a "*new shopping website*" or an "*experimental banking app*," omitting security- or QR code-related terms to minimize bias. The studies consisted of five main parts and started in Qualtrics:

1. Consent, Welcome, & Study Preparation
2. Hands-On Task
3. Task-Specific Questions
4. General Questions about QR Code Usage and Security
5. Wrap-Up & Debriefing

In the following, we provide details on each of these study parts, starting with a description of the "cover stories." The full surveys[2] are linked in Appendix D. Note: General questions were omitted in our small-scale experiment.

[2]Note: Studies were conducted in Germany, so to participants, all study material was available in German only. References to study materials in this paper thus represent translations.

3.1 Cover Stories

3.1.1 Study I – *Shopping*

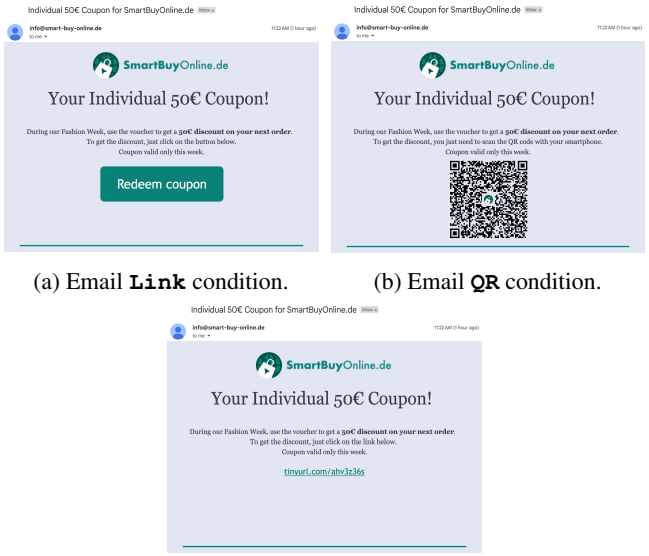
In Study I, our *Shopping* use case, participants tested an online shop and its new AI feature, which we claimed to evaluate shopping orders based on style and cost-effectiveness.

Task Description **'Register & Familiarize with Online Shop'** At first, participants familiarized themselves with the website by exploring its features and functionalities on their own terms (cf. Figure 8a). To do so, they first registered at the website using a personal email address which they were actively using and currently had access to. Following best practices, we subsequently sent a registration confirmation to their inbox, asking them to confirm the registration by clicking the provided link (cf. Appendix B). We did not restrict the device on which users could open the emails. After that, participants were able to log in to their newly created account and were instructed to place a first test order. This allowed us to ensure participants had understood the functionalities of the website and provided us with an email correspondence to send subsequent emails to. Participants could continue with the second part of the study task once they provided their unique order confirmation number in Qualtrics.

'Receive Coupon Email & Place Second Order' In Qualtrics, we introduced the shopping AI feature in more depth, explaining that it would evaluate (i. e., 'score') the chosen outfit of the following second order. We informed participants that they might receive an email with a coupon, but emphasized that this was not guaranteed. To nudge them to check their inbox for potential coupon emails, we claimed they could increase their study earnings by choosing an outfit that receives a high AI score (which supposedly considered cost-effectiveness). Simultaneously, we pointed out that participants were operating in the real world and not in a safe and controlled study environment, meaning they need to beware of online threats such as phishing and scam. Note: In reality, every participant received the same AI score and payment, which we disclosed in the debriefing later.

In the meantime, we sent participants an email containing a 50 € shopping coupon which they could access either by clicking a button in the **`Link`** condition (cf. Figure 1a), scanning a QR code in the **`QR`** condition (cf. Figure 1b), or clicking on a shortened URL in the **`Short URL`** condition (cf. Figure 1c) which we introduced in the small-scale experiment. While participants placed their second order on the shopping website, they were free to interact with the received (malicious) coupon email and website on their own terms.

The Conditions The coupon email and coupon website lay at the core of our experimental study manipulation and differed slightly depending on the study condition. Each participant was assigned to one of the following four conditions:



(a) Email **`Link`** condition. (b) Email **`QR`** condition.

(c) Email **`Short URL`** condition (small-scale experiment).

Figure 1: Coupon email containing a link (button), a QR code, or a short URL (small-scale experiment). The email was sent either by the legitimate web shop *SmartBuyOnline.de* (info@smartbuyonline.de) or a malicious sender (e. g., info@smart-buy-online.de).

1. **`Link`** *control*: Participants who **clicked** on the 'Redeem Coupon'-button are forwarded to a **legitimate** login page to enter their email and password (created for smartbuy-online.de). Then a 6-digit coupon code is displayed.
2. **`Link`** *malicious*: Participants who **clicked** on the 'Redeem Coupon'-button are forwarded to a **malicious** login page, asking them to enter email address and password. Then a *'coupon is invalid'* message is displayed.
3. **`QR`** *control*: Participants who **scanned** the QR code are forwarded to the **legitimate** login page, asking them to enter their credentials. The 6-digit coupon is displayed.
4. **`QR`** *malicious*: Participants who **scanned** the QR code are forwarded to the **malicious** login page, asking them to enter their credentials. The invalid message is displayed.

For **`Short URL`**s, we had the same *control* and *malicious* case, though instead of a button/QR code, a clickable shortened link was displayed. The "*legitimate*" coupon website was hosted on the same domain as our shopping website (*SmartBuyOnline.de*). The *malicious* coupon website was hosted using URLs closely mimicking the shopping website. The URLs were inspired by research that studied real-world phishing URL obfuscation techniques [50, 52]. Specifically, we used a combination of typosquatting,[3] combosquatting,[4]

[3] Typosquatting = adding spell errors or hyphens in malicious URLs.
[4] Combosquatting = combining words e. g., *'legitimate-malicious.com.'*

and adding additional subdomains. The first one used a typosquatted second-level domain (‘*smart-buy-online.de*’), the other used a different top-level, second-level, and additional subdomain, combining typo- and combosquatting (‘*coupon-info-smartbuyonline.couponcampaign.org*’). We varied malicious URLs to minimize wording-related bias.

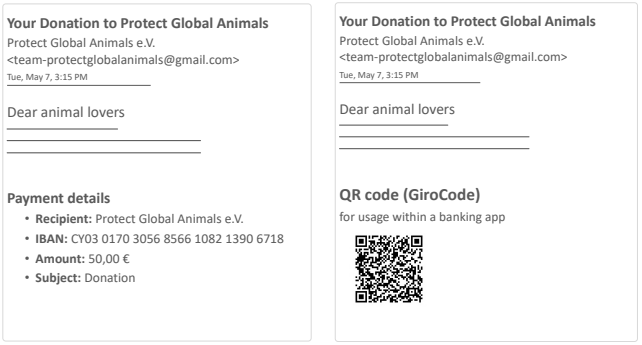
Task-specific Questionnaire Once participants completed their second order, they returned back to Qualtrics where they received their “AI score” and continued with task-specific questions. To capture participants’ general experience with the study task, we first asked about the perceived effort of the registration/login (**S1**) and order process (**S2**). Following that, depending on participants’ behavior in the study, they received slightly different sets of questions. Participants who had redeemed the coupon were asked about the effort of using the coupon (**S3**), to explain why they had used it (**S4**/**S5**), and to indicate how trustworthy they perceived the coupon email (**S6**) and website (**S7**). Participants who had only opened the (phishing) coupon website but did not enter credentials were asked about their reasons (**S8**) and to rate the trustworthiness of the website (**S9**). Participants who had not even opened the coupon website were asked whether they had noticed (**S10**) and read (**S11**) the coupon email. If so, we asked for their reasons for not accessing the coupon website (**S12**) and to rate the trustworthiness of the coupon email (**S13**).

3.1.2 Study II – *Payment*

Our second use case (*Payment*) invited participants to test a (hypothetical) banking app which we made publicly available for Android and iOS through the official app stores.

Task Description ‘Download & Familiarize with App’ Again, we first introduced participants to the study task (‘testing a new online banking app’) via Qualtrics and then instructed them to download the app from the app store (cf. Figure 9a). In Qualtrics, we provided a (individual) PIN to log in to the banking app and familiarize with its functionalities. From the beginning, participants were aware that the app was only for test cases and did not support real transactions. For the tasks we however encouraged them to *imagine* being in a real situation using a real banking account.

‘Perform Transaction’ Next, participants were instructed to transfer a specified amount of money to a certain receiver via the app (cf. Figure 9b). The detailed information about this *scenario* was displayed in an email in subsequent steps of the questionnaire. Before that, we presented the *legitimate* payment details for participants’ scenarios, emphasizing these as the details to transfer the money to. Additionally, we informed them that not all transaction requests are trustworthy (like in real life) and that they should carefully verify whether the payment details in the email match the provided legitimate details. Subsequently, we displayed the promised email in Qualtrics (cf. Figure 2), participants performed the transaction in the app and returned back to Qualtrics to finish the study, answering the *task-specific* and *general questions*. Note: The legitimate payment information was continuously and prominently displayed alongside the email.



(a) Payment **`Text`** condition. (b) Payment **`QR`** condition.

Figure 2: Email from *Payment* use case containing the scenario of a 50 € donation to the organization Protect Global Animals e.V. (scenario *‘Donation’*). The payment details were provided as plain text (2a) or encoded in a QR code (2b).

The Conditions Again, we had four conditions:

1. **`Text`** *control*: The email displays payment details in plain text. These details match the ones we specified as *legitimate*. Participants manually type the information in the banking app.
2. **`Text`** *malicious*: The email displays payment details in plain text. These details **do not** match the ones we specified as *legitimate*. Participants manually type the information in the banking app.
3. **`QR`** *control*: The email displays a QR code. Participants scan the QR code using the app and the details are displayed automatically. These details match the ones we specified as *legitimate*. Participants have the option to manually change the details if they like.
4. **`QR`** *malicious*: The email displays a QR code. Participants scan the QR code using the app and the details are displayed automatically. These details **do not** match the ones we specified as *legitimate*. Participants have the option to manually change the details if they like.

The Scenarios & Payment Details We used four scenarios (donation, streaming, energy bill, package delivery) to prevent results depending on a specific story. We also varied amounts (low, medium, high, very high) and IBANs[5] by randomizing

[5]The European SEPA transfer standardizes payments using International Bank Account Numbers (IBANs) across 36 countries including non Euro-members like Switzerland or Monaco [18].

within the same country code (DE), or using varying length IBANs with different country codes (*GB*–Great Britain, *CY*–Cyprus, *BE*–Belgium). Note: The goal was *not* to analyze differences between scenarios, amounts, or payment details but to minimize potential biases arising from potential associations with them.

Task-specific Questionnaire We first asked participants to assess the perceived effort of the login process (**B1**) and the payment in the app (**B2**). We also asked how secure participants felt during the payment (**B4**) and how trustworthy they perceived the email (**B5**). Lastly, they highlighted aspects that may have stood out to them (**B3**).

3.1.3 General Questions

In the second half of Study I and II, we included an identical set of questions, about participants' general QR code usage and their beliefs about QR code security. First, we investigated participants' perceptions of and experiences with QR codes, asking about the perceived effort (**Q1**), usefulness (**Q3**), and purposes for which they had used them (**Q2**). To learn how participants understand the functionality and security of QR codes and what misconceptions they may hold, we asked them to rate various statements about potential misuse on 5-point agreement scales (**Q5**, **Q17**–**Q20**). We also inquired about the reasons for these believes (**Q7**–**Q9**) and how they think one could identify malicious QR codes (**Q10**). We also collected their experiences with and concerns about (QR code-based) fraud and phishing (**Q11**–**Q13**), and their confidence in detecting different types of online attacks (**Q14**–**Q16**). Lastly, we measured privacy disposition (**Q31**–**Q32**) using validated scales [10, 40]. Both scales (one general and one context-specific for the app/website) measure individual sensitivity to data privacy, i.e., how strongly individuals value protecting their personal information compared to others. Higher scores reflect greater privacy concerns and caution around data handling practices. Finally, we asked about online shopping (**S14**–**S17**) or online banking behavior (**B6**–**B12**), and used the **SUS** (System Usability Scale), to capture potential differences in the perceived usability of the tested conditions. Note: Except for the SUS scale, we did not ask these questions in the small-scale study (**`Short URL`**).

3.2 Recruitment, Demographics & Analysis

We recruited via the panel providers *TalkOnlinePanel*[6] and *Cint*.[7] Participation took 27 and 21 minutes (median) with an hourly compensation of 12.90 € and 8.30 €. As the questionnaire was shorter in the small-scale study, it only took 17 minutes with an hourly compensation of 15 €. Ensured by panel providers, we limited participation to desktop computers and laptops as there is no standardized way to open QR codes directly on mobile devices.

Pilots We piloted the studies via Prolific with 30 participants each (hourly compensation: 14.30 € and 12.80 €). Based on this, we identified a parameter misconfiguration that prevented registration completion for some participants and a display rendering issue on devices with differing screen sizes which we fixed before launching the main studies.

Sample Description After sanitization, we had a total of 1,746 participants, $n = 858$ in the *Shopping* use case and $n = 888$ for the *Payment* study. In both cases, these were about equally distributed across conditions, however, due to filtering participants' who failed the attention check, groups were not exactly equal. Concretely, for *Shopping*, **`QR`** *malicious* and *control*, and **`Link`** *malicious* had $n = 216$ participants, **`Link`** *control* had $n = 210$. For *Payment*, both **`QR`** groups had $n = 222$, **`Text`** *control* had $n = 223$ and **`Text`** *malicious* had $n = 221$. For the small-scale experiment (**`Short URL`**), we recruited $n = 130$ participants, equally distributed into *control* and *malicious* condition ($n = 65$ each).

Samples in the original studies were representative according to age and gender. Lower education was underrepresented (10% in studies vs. 29% in population). The small-scale experiment was representative according to gender but skewed slightly towards younger and highly educated participants. The full demographics are listed in Table 1.

Quantitative Analysis We analyzed responses to open-ended questions using an iterative coding process. Two researchers independently coded the first 20% of responses, then combined their codebooks through discussion. Responses were recoded based on this unified codebook, with inter-rater reliability (Cohen's Kappa) of at least $\kappa = 0.81$. A third researcher coded the remaining responses. The codebooks can be found in the extended version [34].

Qualitative Analysis Our key figure is the measured *susceptibility* to the phishing (Study I) and scam (Study II) attacks. In both studies, susceptibility is represented by the difference between the malicious conditions (**`Link`**/**`Text`** *malicious* vs. **`QR`** *malicious*). In Study I (*Shopping*), participants "fell for the phishing" if they entered their login details on the coupon website **and** "used the coupon." In Study II, participants "fell for the scam" if they used the malicious payment details displayed in the email, instead of the legitimate ones. We also ensured that secondary factors (e. g., perceived trustworthiness, usability of website/app) did not cause measured differences. Using regression analysis with stepwise model selection, we investigated the influence of other factors like demographics, beliefs about QR codes, and privacy disposition. However, model fit for *Shopping* was low. Regression models can also be found in the extended version [34].

[6] TalkOnlinePanel: www.talkonlinepanel.com, as of June 12, 2025
[7] Cint: www.cint.com, as of June 12, 2025

3.3 Limitations

Realism of Study Use Cases We designed our studies to mimic real-world phishing and financial scam as closely as possible. In Study I, participants received actual emails sent to real email addresses on their personal devices. In Study II, they downloaded a fictional but plausibly designed online banking app and logged into a user-specific account. Despite these efforts, the studies were still conducted in a controlled experimental environment. The accounts used likely did not carry the same personal value as participants' real-life accounts. Additionally, mentioning online threats at the beginning of the studies may have influenced participants' vigilance compared to everyday situations. However, this step was essential to prevent participants from automatically trusting all study-related content. Other aspects such as the email content's association and temporal connection to the studies may have influenced participants' susceptibility further compared to real life. However, we kept our emails as generic as possible to minimize this risk. Our primary goal was to compare susceptibility rates between QR codes and links/text under controlled conditions. Given this comparative focus, we consider these deviations from real-life acceptable. We do not claim that our measured rates reflect real-world behavior.

General Limitations Due to our study setup, participants' responses to the general questions about QR codes may have been partially influenced by their interaction with the study tasks. Additionally, since our studies were conducted only in Germany, the results may not fully generalize to other populations. The studies' resource-intensive and organizationally demanding setups (i.e., large samples, technical complexity) confined our ability to expand the sample to multiple populations. However, considering that Germans are typically known as privacy-cautious [37], we expect the results to represent a lower bound at worst. Nonetheless, studying the same topic in other countries and cultures is highly desirable and should be investigated in future work. Unfortunately, participants with lower education were slightly underrepresented. As education can influence risk perception and interaction with (security) technology this may have affected susceptibility in two opposing ways: (i) fostered overconfidence to detect malicious emails, increasing susceptibility [8], or (ii) increased overall awareness and digital literacy, thereby lowering susceptibility rates [64]. Lastly, since Study I and the small-scale experiment were conducted one year apart, participants' opinions and perceptions may differ slightly due to changes in public awareness or relevant news over time.

4 Results

In this section, we present the results of our experimental studies, as well as our general questions about participants' understanding of QR code-based security threats.

Table 1: Participant demographics in online surveys.

	Shopping				Payment	
	Original $n = 858$		Short URL $n = 130$		$n = 888$	
	n	**%**	**n**	**%**	**n**	**%**
Gender						
Female	433	(50.5 %)	68	(52.3 %)	441	(49.7 %)
Male	423	(49.3 %)	61	(46.9 %)	445	(50.1 %)
Non-binary	2	(0.2 %)	1	(0.8 %)	2	(0.2 %)
Age						
18–29	163	(18.3 %)	21	(16.2 %)	163	(18.3 %)
30–39	165	(18.5 %)	34	(26.2 %)	165	(18.6 %)
40–49	156	(17.6 %)	45	(34.6 %)	156	(17.6 %)
50–59	197	(21.9 %)	14	(10.8 %)	203	(22.9 %)
60–74	212	(23.6 %)	16	(12.3 %)	201	(22.6 %)
Education[a]						
Low (*ISCED 0-2*)	88	(10.3 %)	3	(2.3 %)	90	(10.1 %)
Medium (*ISCED 3-4*)	324	(37.7 %)	35	(26.9 %)	366	(41.2 %)
High (*ISCED 5-8*)	446	(51.9 %)	92	(70.8 %)	432	(48.6 %)
Background						
Technical	371	(43.2 %)	67	(51.5 %)	399	(44.9 %)
Non-Technical	481	(56.1 %)	61	(46.9 %)	483	(54.4 %)
Prefer not to answer	6	(0.7 %)	2	(1.5 %)	6	(0.7 %)
Privacy Disposition						
Mean (SD)	3.23	(0.82)	3.15	(0.78)	3.28	(0.74)
Website/App Privacy[b]						
Mean (SD)	3.17	(0.96)	3.05	(1.13)	3.23	(0.89)
Experienced Fraud						
Yes	210	(24.5 %)	-	-	229	(25.8 %)
No	572	(66.7 %)	-	-	581	(65.4 %)
Unsure	68	(7.9 %)	-	-	73	(8.2 %)
Experienced QR Fraud						
Yes	9	(1.1 %)	-	-	3	(0.3 %)
No	815	(94.9 %)	-	-	848	(95.5 %)
Unsure	30	(3.5 %)	-	-	36	(4.1 %)
Send Money Wrong						
Yes	-	-	-	-	103	(11.6 %)
No	-	-	-	-	769	(86.6 %)
Unsure	-	-	-	-	14	(1.6 %)
Experienced Phishing						
Yes	93	(10.8 %)	-	-	-	-
No	628	(73.2 %)	-	-	-	-
Unsure	135	(15.7 %)	-	-	-	-

[a] Education classification based on UNESCO ISCED 2011. Low = High school or below. Medium = university entrance qualification or occupational/vocational training. High = technical/admin./professional degree, Bachelors', Masters', and PhD.
[b] *Website* privacy in shopping, *app* privacy in payment use case.

4.1 Susceptibility to QR Code Threats (RQ 1)

First, we address our main research question, the susceptibility to QR code-based attacks (RQ 1). We individually report the studies' results, always comparing participants' detection rate with QR codes to the detection rate with the traditional method: **`Link`** in the shopping use case and **`Text`** in the payment use case. We also report the results for **`Short URL`**.

4.1.1 Online Shop

In the shopping use case, participants received an email informing them about a coupon for their order. This coupon could be accessed by scanning the QR code in the email (**QR**), by clicking on the button (**Link**), or on the shortened link (**Short URL**). Additionally, QR code, link, and short URL were either *malicious* or legitimate, the latter being our *control* group. We measured both how many participants opened the coupon website, i.e., clicked on the button/link or scanned the QR code in the email ("website opened"-rate), and how many actually entered their login details on the coupon website to retrieve the coupon code ("coupon used"-rate). The latter would be a real attacker's end goal, trying to steal login credentials. We therefore consider only participants who opened the coupon website **and** entered their login credentials in the *malicious* case to have fallen for the phishing. Table 2 summarizes participants' interactions with both the email and the coupon website for all conditions.

Table 2: Interactions with the coupon email and website.

	Seen Mail		Read Mail		Opened WS		Used Coupon		Total
Link									
Control	179	(85.2%)	174	(82.9%)	160	(76.2%)	158	(75.2%)	210
Malicious	171	(79.2%)	164	(75.9%)	99	(45.8%)	93	(43.1%)	216
QR code									
Control	181	(83.8%)	174	(80.6%)	120	(55.6%)	118	(54.6%)	216
Malicious	177	(81.9%)	165	(76.4%)	115	(53.2%)	107	(49.5%)	216
Short URL									
Control	50	(76.9%)	48	(73.8%)	23	(35.4%)	23	(35.4%)	65
Malicious	55	(84.6%)	53	(81.5%)	23	(35.4%)	22	(33.8%)	65

General Interaction with Email & Coupon The vast majority of participants have seen the coupon email (81%) and consequently read it (78%). This was equally true for all conditions. 76% of participants in the *control* group of the **Link** condition opened the coupon website (cf. Figure 3) and used the coupon for their order (75%). Compared to that, significantly fewer participants in the **QR** *control* group opened the coupon website (56%) and used the coupon (55%) ($\chi^2(1) = 18.93, p < .001, V = .22$). Scanning the QR code requires substantially more effort as it entails using an additional device, potentially even grabbing it from a different location (instead of just clicking on a link). Therefore, this result is unsurprising. In line with that, 29 out of the 56 participants who chose not to use the coupon in the **QR** *control* condition reported convenience issues as the reason.

Surprisingly, even fewer participants opened the website in the **Short URL** *control* condition (only 35%). There is no clear explanation for this finding with the majority of participants simply stating it *"wasn't necessary"* [SU-40] or *"already ordered"* [SU-129] as the reason for not clicking the link. Three participants indicated they distrusted or felt uncomfortable clicking on, especially shortened links, though this was a minority.

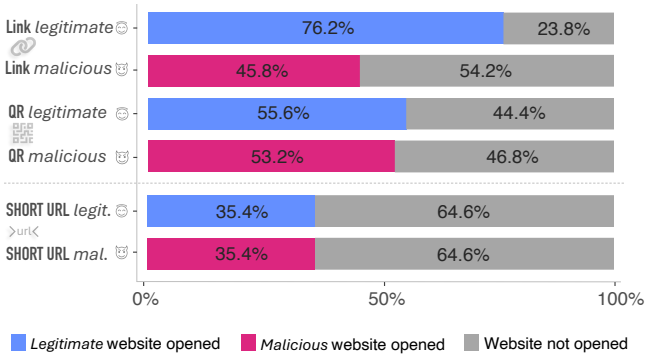


Figure 3: Participants' susceptibility to phishing in Study I (*Shopping*). Plots show participants who opened the coupon website by clicking on the link, the short URL, or scanning the QR code in the coupon email.

Susceptibility to Phishing To determine the difference in susceptibility, we compare the "website opened"– and "coupon used"–rates of the *malicious* groups of the QR code and link condition.

46% of participants in the **Link** condition opened the website and 43% subsequently used the coupon. In the *malicious* **QR** condition, 53% opened the website by scanning the QR code and 50% consequently used the coupon. This difference of around 7% (**Link** *malicious*: 43% vs. **QR** *malicious*: 50%) initially seems very small and is not significant ($\chi^2(1) = 1.57, p = .210, V = .06$). However, this difference mostly ties back to the overall much lower baseline of participants willing to scan the QR code than to click the link in the first place. Comparing the "coupon used"–rates within each method (**Link** *control* vs. *malicious* and **QR** *control* vs. *malicious*) clearly shows that participants were able to identify the phishing in the **Link** condition, 75% had used the coupon in the *control* condition whereas only 43% did so in the *malicious* condition ($\chi^2(1) = 44.24, p < .001, V = .33$). Contrary to that, there is almost no difference in the "coupon used"–rates of the **QR** groups (*control*: 54% vs. *malicious*: 50%; $\chi^2(1) = 0.93, p = .336, V = .05$) which indicates little awareness about the possibility of using the QR code maliciously. In the **Short URL** condition, we saw a similar pattern as with the QR code with basically no difference between the *control* (35%) and *malicious* (34%) condition ($\chi^2(1) = 0, p = 1, V = .01$). As the number of participants who opened the website and used the coupon was already low overall it is difficult to clearly attribute these findings.

The above observations are also reflected in the open answers. In the *malicious* **Link** case, 26 out of 71 participants identified the mail as phishing, e. g., saying *"phishing attempt"* [S-24], *"wrong sender"* [S-25], *"the address is similar but with a hyphen, so it's not the original"* [S-58]. In the **QR** case, only 2 out of 58 participants reported recognizing the phishing attempt: *"The email seemed phishy to me - pun intended. The*

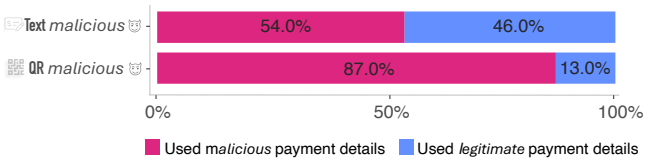


Figure 4: Distribution of participants who did and did not use the malicious payment details ('fell for the scam') in Study II (*Payment*). Participants saw payment details in human-readable format (**`Text`**) or received a payment QR code (**`QR`**).

sender of the email (@smart-buy-online.de) did not match the sender of the registration email (@smartbuyonline.de)" [S-873], *"because the website to redeem the coupon did not match the original site, I chose not to sign up"* [S-405]. Despite no measurable difference in the "coupon used"-rates, the open answers for **`Short URL`** reflected a similar picture as those of the **`Link`** condition with 12 out of 30 participants mentioning phishing as their reason for not using the coupon in the *malicious* case (*"the short link seemed suspicious to me"* [SU-13], *"the sender was not correct"* [SU-49]).

4.1.2 Online Payment

To investigate the results of the *payment* scam, we now compare the **`Text`** *malicious* to the **`QR`** *malicious* group. Note: Everyone in the *control* condition used the legitimate payment details, as participants had no choice of whether or not to use them like they had in Study I. In the **`Text`** *malicious* condition, where participants typed the payment details manually, 101 out of 221 participants (46%) used the correct (non-malicious) banking details (cf. Figure 4). As the open answers reveal, almost everyone did so because they noticed that the banking details in the email differed from the ones we deemed as "correct," for example saying, *"the IBAN provided in the email does not align with the correct IBAN (green field)"* [P-324] and *"the IBAN did not match the verified IBAN from the official website"* [P-874]. In comparison to that, only 29 of 222 participants in the **`QR`** condition used the non-malicious details meaning only 13% of participants recognized the QR code-based fraud. This ratio of participants who recognized the fraud significantly differs between the **`Text`** and **`QR`** groups ($\chi^2(1) = 55.34, p < .001, V = .36$).

4.1.3 Factors Influencing Susceptibility

Using logistic regression, we further investigated factors influencing participants' susceptibility (cf. regression results in the extended version [34]; *Shopping*: $R^2 = 0.09$, $\chi^2(15) = 25.89, p = .04$; *Payment*: $R^2 = 0.29$, $\chi^2(11) = 50.56$, $p < .001$). Despite related research showing relationships between experience with fraud and caution online [45], in our case, prior experience with fraud (Q12) did not show any influence in either use case, reinforcing the impression that users are not sensitized to QR codes as an attack vector. Participants who did not believe that QR codes can contain malicious content in the Payment use case (Q5) were significantly less likely to recognize the forge ($\beta = -1.38, p < .001$). This underlines the importance of raising awareness about the topic overall, as someone who does not believe that QR codes can be misused in the first place will consequently be unable to protect themselves as well. Demographic variables, including technical background, showed no significant influence in both studies. Only privacy disposition in the *Shopping* use case ($\beta = -0.48, p < .05$) and app privacy scores in the *Payment* use case ($\beta = 1.22, p < .01$) significantly correlated with susceptibility.

4.1.4 Validity of Study Use Cases

To ensure our results reflect differences in the ability to recognize fraud and are not influenced by unintended variations in the study design, we assessed both the perceived effort required for different study tasks and the perceived trustworthiness of the emails and websites participants interacted with. All values were measured on 5-point Likert scales, with five being the highest effort and trustworthiness rating respectively. SUS scores range from 0 to 100.

Effort. For *Shopping*, across all three conditions, effort ratings for *account registration* ($m = 1.5$, $sd = 0.8$) and *ordering on the website* ($m = 1.6$, $sd = 0.8$) were low. The SUS scores were in the "good" range (76, $sd = 15.4$) [65]. The effort rating for *using the coupon* was overall low as well ($m = 1.9$, $sd = 1.1$), however using the QR code was perceived significantly more effortful than using the regular link ($\chi^2(2) = 25.07, p < .001$; posthoc Bonferroni-corrected Wilcox: **`Link`** vs. **`QR`** $p < .001, r = .30$). There were no statistical differences between **`Link`** and **`Short URL`** and **`QR`** and **`Short URL`**. For *Payment*, the effort ratings for the *login* were even lower ($m = 1.4$, $sd = 0.8$), and the SUS score was 81 ($sd = 16.2$). The *transaction* effort ratings were equally low ($m = 1.6$, $sd = 0.9$), however, this time using QR codes was rated as *less* effortful than manual typing ($W = 116203, p < .001, r = .18$).

Perceived Trustworthiness. For *Shopping*, 60% rated the email as trustworthy ($m = 3.5$, $sd = 1.1$). Similarly, the trustworthiness of the coupon website was high ($m = 3.5$, $sd = 1.1$). For *Payment*, the trustworthiness of the email was mediocre ($m = 3.1$, $sd = 1.2$) and the majority indicated that they felt secure when performing the transaction in the app ($m = 3.7$, $sd = 1.0$).

Influence of URL. In the *Shopping* use case, we used two different malicious URLs to dilute the explicit influence on the susceptibility. To ensure there was in fact no difference, we compared the "coupon used"-rates within the *malicious* groups. For **`Link`**, 49% used the coupon with the "hard" URL whereas only 38% used it with the "easy" URL. This difference however is not signifi-

cant ($\chi^2(1) = 2.23, p = .136, V = .11$). For **QR**, 48% used the coupon with the "hard" URL, 51% used it with the "easy" URL ($\chi^2(1) = 0.07, p = .787, V = .03$). For **Short URL**, 44% used the coupon with the "hard" URL and 22% with the "easy" URL. Again the difference is not significant ($\chi^2(1) = 1.97, p = .16, V = .21$).

4.2 Strategies to Detect Malicious QR Codes (RQ 2)

Across Study I and II, we asked participants to explain how they would try to recognize malicious QR codes. Of all 1,746 participants, 694 cited a '*lack of knowledge*,' suggesting that these participants either struggled to explain how to identify malicious QR codes or were entirely unsure of how to verify their legitimacy. Furthermore, 25 participants explicitly stated they lacked sufficient experience with malicious QR codes on how to recognize them *"I don't know, unfortunately, I haven't had any experience with that"* [P-12], while 16 explicitly indicated they need more information on the subject *"I don't know, I need to find out first"* [S-550].

340 participants, the second largest group, believed distinguishing malicious QR codes from legitimate ones is impossible *"I think, as a non-expert, not at all"* [P-214]. 221 participants proposed scanning the QR code to verify its encoded content, with 274 specifically referencing the context (use case) of opening URLs *"if you are directed to a suspicious website; check the URL"* [P-90; P-133]. At first glance, this approach of verifying the data the QR code encodes seems reasonable, however, our findings from both use cases indicate that users often fail to perform thorough verification of the underlying encoded data.

186 respondents expressed trust in a QR code as long as its source is perceived as reliable *"... but if the source of the code is reliable, it should be alright"* [P-3]. Though this is the most reliable strategy for verifying a QR code's legitimacy before scanning it, it raises concerns we further discuss in Section 5.3. 62 participants reported placing their trust in the security features of their smartphone, even though most built-in scanner apps do not provide any security features for QR codes. Notably, 30 participants mistakenly cited a supposed 'distinct visual appearance' of legitimate QR codes as a sign of authenticity, which might be true for physical QR codes but cannot be applied to digital ones *"the QR code will appear unusual, such as having incomplete edges; the QR code looks altered; structure"* [S-12; S-149; S-165].

4.3 Experiences with Malicious QR Codes (RQ 3)

Next, we assess participants' past experiences with QR fraud, their concern about it, and their confidence in detecting it.

Experience with QR Fraud Despite about 25% of participants having fallen victim to online fraud in general (Q12), almost no one reported having knowingly experienced QR code-based fraud (∼95% no QR fraud experience, Q13). This may have two reasons: (1) the attack type is still relatively new and attackers are only starting to explore their possibilities, which is underlined by a recent rise in news outlets warning about this attack type [14, 25, 43, 46]. (2) Users are more oblivious to this than to other types of attacks making it particularly difficult to identify malicious QR codes.

Concern About QR Fraud Possibly in consequence of few encounters with forged QR codes, participants were only mildly concerned about malicious QR codes (Q6). The majority, about 72%, indicated being slightly or moderately concerned, with an average rating of 2.8 ($sd = 0.98$).

Confidence Detecting QR Fraud Despite indicating relatively high confidence to detect traditional fraud (Q14), or phishing (Q15), participants were rather uncertain about their ability to detect QR code fraud (Q16). About 33% each rated their confidence as extremely low, very low, or moderate. Barely any participant was more than moderately confident, which already indicates that users are aware that they have little ability and knowledge about how to determine the legitimacy of a QR code and are not well-equipped to protect themselves from QR code-based attacks.

4.4 Beliefs About QR Code Security (RQ 3)

Next, we report how participants perceive the potential for misuse of QR codes in general (Q5–Q9 and Q17–Q20).

4.4.1 Belief that QR Codes Contain Malicious Content

First, participants were asked to indicate their agreement with the statement "QR codes may contain fake information" on a 5-point scale (Q5). Encouragingly, Figure 5 shows that the majority leans towards agreeing with the statement, correctly believing that QR codes in fact can contain malicious content. While about 45% "moderately" agreed, indicating to be rather uncertain, almost 20% were fully certain that QR codes can be malicious. In the following, we thoroughly investigate participants' reasoning for or against believing that QR codes can be forged based on their open answers (Q9).

'QR codes are forgeable' The most frequently cited reason for believing that QR codes can be forged is their nature of "concealing" the underlying data (226 out of 733 participants), indicating that many participants intuitively recognized the potential security threats associated with their use. In total, 94 participants expressed general distrust toward anything online, regardless of whether QR codes were involved, while 33 responses specifically indicated a lack of trust in QR codes, i. e., saying they have *"limited control over the authenticity of QR codes"* [S-80]. 88 participants acknowledged the ease with which QR codes can be generated by anyone, which is true for the majority of common QR code use cases, reflecting that there is at least a basic level of technical awareness

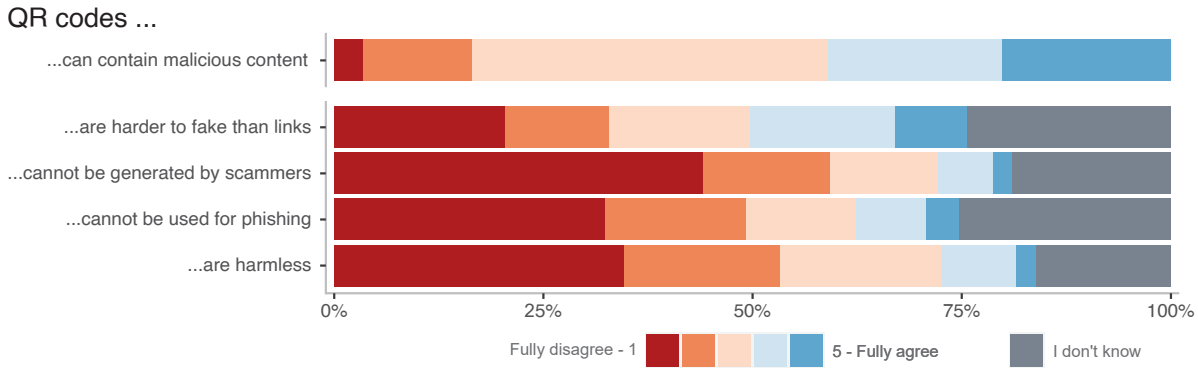


Figure 5: Participants' agreement to statements about QR codes' security and potential misuse. Statement 1 (Q5) is considered true, correct answers on the right. Statements 1–4 (Q17–Q20) are considered false, correct answers on the left.

about how QR codes are generated among this group *"generating QR codes yourself is easy these days..."* [S-108]. A substantial number of participants highlighted the concealed nature of the URL (84 responses) *"I can embed fraudulent links in QR codes"* [P-647], followed closely by concerns about phishing (82 responses) *"QR codes can be generated by scammers and lead to websites that may involve phishing. You can't tell this from the QR code itself"* [S-507]. This suggests that many participants directly associate QR codes with website access and recognize the potential risks stemming from URL obfuscation, however, they also seem to disregard other applications of QR codes and the associated risks.

Participants who expressed uncertainty in Q5 (being unsure) regarding whether QR codes could contain malicious information predominantly cited a lack of knowledge about the functionality and properties of QR codes (123 of 771 participants). This group also exhibited a broader sense of distrust toward online environments or indicated higher caution due to the prevalence of cybercrime (149 responses). Similar to those who believed that QR codes can contain false information, many participants in this group emphasized the obfuscating nature of QR codes (147 responses). At least 40 participants correctly argued that the likelihood that a QR code contains malicious content depends on the context, use case, and the credibility of its source.

'QR codes are not forgeable' Many participants who thought that QR codes cannot contain malicious information argued that they never heard of malicious QR codes (27 out of 296 participants) or never had negative personal experiences with them (23 responses). 28 participants perceived that QR codes convey a *"sense of security; You can never be 100% sure, but I have a general trust in the codes"* [P-341; P-462], indicating a potentially dangerous trust in the QR codes. Some participants (26 responses) believed that the distinct appearance of QR codes ensures their security, while others incorrectly asserted that QR codes are secure by design (22 responses) *"in today's times, the codes are protected. I trust their security; a lot of technology and skill are involved in a QR code"* [S-303; S-608]. However, in most use cases, QR codes merely encode information (like URLs or payment details) and do not have any inherent security features by default. Whereas 88 participants who considered QR codes as potentially malicious recognized that QR codes are easy to generate, 21 participants in this group argued that creating malicious QR codes would require too much effort, which is why they (supposedly) cannot contain malicious content – again, a misconception in most use cases. Additionally, 16 responses emphasized the (visual) complexity of QR codes *"too complex design"* [P-894], mistakenly suggesting that this complexity makes them difficult to forge.

4.4.2 Further Beliefs about QR Code Security

Participants also indicated their agreement to further statements about QR codes' security and potential misuse on 5-point Likert scales (Q17–Q20). To avoid forcing participants towards an answer, we additionally provided an option to select "I don't know" for those who were entirely unsure. Figure 5 summarizes these results.

Only 33% were sure that QR codes "*can be used for phishing*" (Q19). Similarly, only 35% fully disagreed with the statement that "*QR codes are harmless*" (Q20). A lot more participants, 44%, were certain that "*scammers **can** generate QR codes*" (Q18). However, a total of 16% up to 25% across all statements indicated being completely unsure. Additionally, between 9% to 12% even indicated full agreement meaning that they believe scammers *cannot* create QR codes, QR codes *cannot* be used for phishing, and that they are overall harmless. Given that participants could choose "I don't know," their choice was likely not just a "wrong guess."

Answers to question Q17, which asked whether *"QR codes are harder to fake than clickable links,"* showed a slightly different distribution. Even fewer participants than in the other statements fully disagreed (21%), and a quarter selected "I don't know." We do, however, acknowledge that this difference might have been caused by ambiguous question-wording.

Participants may have judged this statement from the perspective of generating QR codes "by hand." In that case, it would be true that generating a QR code is harder than generating a link, as malicious links can be created without additional tools while creating QR codes requires some sort of technical assistance. Nonetheless, from an attacker's perspective, this difference in effort is absolutely negligible.

Explicit Misconceptions Some participants had explicit misconceptions, for example, believing that a company logo in the QR code signifies its trustworthiness and authenticity *"especially when there is an image included, I find [QR codes] very trustworthy (it has to match the company)"* [S-554] and *"some QR codes have an image in the center"* [P-75]. Others cited their widespread adoption as 'evidence' for security, conflating usage with trustworthiness. Lastly, some wrongly believed that QR codes are somewhat 'secure by design' or that smartphones and computers have built-in security features, indicating a false trust in the technology.

5 Discussion

Across three experiments, we studied users' susceptibility to malicious QR codes online. Next, we discuss our findings, focusing on the impact of users' (un)awareness regarding malicious QR codes and derive design implications for QR code applications aimed to assist users with safe interactions with QR codes across use cases.

5.1 Influence of QR Codes on Users' Susceptibility to Phishing and Scam (RQ 1)

Our primary goal was to measure how replacing traditional attack "payloads" (like links) with QR codes influences users' susceptibility to common online attacks. In our *Payment* use case, using QR codes instead of human-readable payment information, increased the likelihood of proceeding with a malicious transaction by 33%. Users praised the convenience of simple scanning and appreciated not having to enter payment details manually, but remained unaware of the attack. This suggests that users implicitly trust the correctness of the data encoded in QR codes, leading them to complete transactions without verifying the payment details.

In the *Shopping* use case, at first glance, the difference in susceptibility was not as pronounced. Only about 7% more participants fell for the phishing attempt in the **QR** than in the **Link** condition. However, this seemingly small difference was largely caused by participants' convenience-driven lower likelihood to scan the QR code than to click on the link. Though many users in the **Link** condition detected the phishing attempt, users in the **QR** condition were entirely oblivious to it, underlining the "awareness" gap.

In the small-scale study with **Short URL**s, the *overall* click rate was notably lower than with **Link** and **QR** codes (only about 33%), without a clear explanation for this difference. Susceptibility patterns resembled those of QR codes: minimal difference in click rates between the *legitimate* and *malicious* condition. Nonetheless, participants pointed out phishing in the open answers of the *malicious* group, similar to the **Link** condition. Overall it seems that short URLs are less effective in deceiving users to click, as they are generally reluctant to click on them even in a legitimate scenario.

In summary, users' interaction differs substantially between links and QR codes. While this only partially translates into increased susceptibility, it is almost certain that someone falls for a QR code-based attack once they have been convinced to scan it. Additionally, users' incentive to "go the extra mile" of retrieving the phone is likely higher in real life than in our study context. Lastly, despite users' lower motivation to scan the QR code, attackers have two main incentives for using QR codes nonetheless: (1) Phishing awareness for link-based attacks has improved substantially in recent years and thus convincing users to click on links will likely become increasingly difficult. (2) As users seem to place trust in the QR codes themselves using convincing wording to nudge them to scan may be easier. Considering special cases where users have to decide how to react under time pressure or in the case of spear phishing, where the email is crafted particularly believable, this is even more plausible.

5.2 Beliefs & Misconceptions About QR Codes (RQ 2, RQ 3)

Beyond the measured susceptibility, our open questions reinforced the impression of a lack of awareness and additionally uncovered gaps in skill and ability to identify malicious QR codes. While many participants correctly understood that QR codes encode or "mask" data, many were entirely unsure whether QR codes could be misused for phishing and how easily scammers could exploit them. 20% even believed that it is completely impossible to identify malicious QR codes and nearly 40% acknowledged lacking sufficient knowledge about them. These self-reported knowledge gaps likely contributed to the high level of susceptibility.

Users also doubted their ability to detect QR code-based attacks, reporting low confidence in detecting QR code phishing and scam. Low confidence and a lack of perceived self-efficacy are known to directly influence the performance outcome – meaning if someone believes in their ability to be successful at something they are more likely to achieve it and vice versa. Accordingly, the low success rate is likely influenced by users' lack of confidence [1, 2, 55].

Across the studies, we also identified several, partially dangerous misconceptions. Some believed that QR codes are 'secure by design,' convey a 'sense of security,' or that malicious QR codes would visibly differ, e.g., having no logo.

These findings echo previous research where some users mistakenly relied on perceived security indicators like logos, or authentic design cues on websites and in emails [13, 68]. Leveraging visual differences as an explicit security measure like Bekavac et al. explored for physical QR codes [3], may be an interesting avenue in the online context as well. Additionally, research should investigate measures to protect users from deceptive elements, like branded color schemes, or logos functioning as false trust indicators.

5.3 Varying Threats in Varying Contexts

In the open answers, users primarily associated QR codes with opening URLs to access websites, overlooking the broad range of possible applications. Additionally, the risks tied to different QR code applications vary substantially, making it particularly hard for users to determine the "correct" way to interact with them. This limited understanding is further complicated by the uniform appearance of QR codes, regardless of their purpose. It is impossible to assess its legitimacy through visual inspection alone, leaving users with two primary strategies to assess their trustworthiness: i) relying on contextual factors as trust anchors and "proxies" for legitimacy, or ii) scanning the QR code and carefully assessing its "destination" before interacting further. While the first approach – using contextual trust anchors – can be effective in some cases, it has notable limitations. For example, in offline scenarios even trusted contexts (like a trusted vehicle charging station) can display a malicious physical QR code [14]. Similarly, in online environments, trusted platforms (e. g., legitimate news websites) might unknowingly host malicious QR codes through third-party ads, exposing users to risks like *malvertising*. Still, thoroughly investigating the context of the QR code can serve as an initial indicator of potential threats without exposing users to the risks of scanning the QR code directly.

The second approach – rigorously investigating the QR code destination is not inherently problematic either. Just opening a phishing website does not cause harm itself, only entering secret details becomes harmful. Unfortunately, research consistently shows that once users have been convinced to access a (phishing) webpage, the vast majority (almost 80%) also proceeds to enter their details [39, 62]. Therefore, it is likely that once users have been convinced to scan the QR code, they will also proceed to interact with the malicious service in a harmful way. This is even reflected by our results, where less than 4% opened the (malicious) coupon website without entering their details. Additionally, certain QR codes do pose risks immediately after being scanned, e.g., triggering automatic malware downloads [7]. Lastly, thoroughly investigating a QR code's destination requires significant user attention and technical ability – expectations that are neither realistic nor fair to place on users.

In summary, given the diverse applications of QR codes, context-specific guidance is essential to ensure safe interactions. While sharing a QR code that encodes a URL is generally harmless, sharing a vaccination record or event ticket can reveal private information, like health data or PII. Developers and service providers should ensure that such "specialized" QR codes are accompanied by clear, accessible guidance on their safe use to reduce user's reliance on guesswork and minimize vulnerabilities stemming from a lack of information.

5.4 Design Implications & Recommendations

Based on our findings, we discuss design implications and contextualize recommendations from related work.

Present Relevant URL Information Early research by Krombholz et al. recommended drawing users' attention to critical URL parts, like the second- and top-level domain [36]. While modern QR code scanners generally support this, users fall for malicious QR codes nonetheless. Hence, this practice can serve as a baseline, but applications should provide additional information for users to assess the legitimacy of QR code content, as it is impossible to determine legitimacy without it. This includes resolving shortened URLs in real-time (*'tinyurl.com/usenix2025'* → *'www.usenix.org/...'*) [36].

Interrupt the Flow When scanning a QR code, the encoded content is typically shown and processed immediately. This entices quick, convenience-driven engagement with the QR code, leaving little time to evaluate the legitimacy of its content [59]. Introducing a brief delay before users can interact with the QR code further, may act as a critical buffer, preventing premature interaction with unknown and potentially untrusted environments and instead allows users to focus their attention on reliable security indicators. In other contexts, short delays have already proven effective, i. e., Gerber et al.'s timer nudge effectively increased the time users spend engaging with tracking consent notices [22] and focusing users' attention on the URL for several seconds positively affects their ability to recognize phishing domains [42].

Concretely, we see two promising directions. First, *subconscious delays*, brief enough to go unnoticed (and therefore not be perceived as technical errors), could give users a moment to detect inconsistencies, prompting a sense of "something is off, let me check again." Second, *intervention prompts*, longer delays paired with visual cues, like highlighting critical URL or content parts could *explicitly* attract users' attention for closer inspection. Determining their effectiveness and concrete implementation details (e.g., content to highlight, length of delay) however requires further research.

(QR)-Phishing and Awareness Training? Phishing and awareness trainings are currently the primary approach to educating users about common online attacks. Extending this to address awareness gaps around QR codes would be an

obvious recommendation. While recent work showed that trainings can indeed decrease users' phishing susceptibility [30, 41, 51], other research highlights drawbacks in real-world environments, i. e., disproving their sustainability over longer periods [39, 51] or criticizing the emotional stress they impose on employees in organizational contexts [56].

Adding to this, our findings show that changing only one variable (namely the way the malicious information is displayed – QR code instead of link) can prevent users from applying their previous knowledge about phishing. This suggests that even small changes in the way an attack is framed can make existing training ineffective, raising doubts about the (long-term) value of those programs.

Context-Dependent Awareness Given the variety of threats, abstract training alone is insufficient to raise user awareness. App developers should prioritize proactive strategies to educate users on secure QR code use. Scanner apps could provide context-specific information (i. e., using icons), such as reminding users to verify recipient details for payment QR codes. Similar to web browsers and email clients, warning users about phishing, QR scanner apps could additionally increase awareness by displaying warnings for deny-listed sites, as suggested in previous research [35, 48].

5.5 Future Work

Influence of QR Code Characteristics. Our research highlights the general risks of QR codes and users' lack of awareness. However, we did not examine which specific characteristics of QR codes make them effective in deceiving users. Future work should explore how masking properties (e. g., text-based masking via short URLs vs. image-based masking with QR codes) and design elements (e. g., trusted logos, and color schemes) affect user perception and susceptibility. This helps deepen the understanding of visual trust cues and informs developing effective interventions.

Technical Defenses. Rather than relying on users to assess the content and origin of QR codes, technical solutions should be prioritized. To identify effective approaches, future research should examine their usability trade-offs and potential side effects (e. g., testing effects of delay durations, highlighting methods, warnings, or real-time resolution).

Cross-Country Comparison. QR code adoption and use cases differ substantially across countries (i. e., widespread use of QR code-based payments in Asia, e. g., AliPay, WeChat Pay). Cross-country studies could yield valuable insights into contextual factors affecting the perception, knowledge, and misconceptions about QR codes.

6 Conclusion

QR codes, commonly used to facilitate human-computer interaction, can amplify traditional threats like phishing and financial scam. Our user studies with 1,876 participants reveal that users lack of knowledge regarding the characteristics of QR codes and are unaware of their potential for misuse. Many participants falsely assume QR codes are secure and trust them despite being aware of their limited knowledge and experience. This lack of understanding hinders their ability to distinguish legitimate QR codes from malicious ones. In response, we propose design recommendations for applications with built-in or third-party QR scanners to help users detect suspicious activities.

7 Ethics Considerations

When we conducted both studies, our department did not have an institutional review board (IRB), and the existing IRBs at our institution were limited to reviewing medical studies and do not cover our type of research. We strictly followed best practices of human subject research (in accordance with the *Menlo Report*) and applicable data protection guidelines [66]. We complied with the EU's General Data Protection Regulation (GDPR) and obtained participants' informed consent at the beginning of the study. Additionally, as our study involved deceptive elements, we thoroughly debriefed participants in the end. First, we revealed the true purpose of the research and highlighting our real intentions. Participants could then choose to withdraw from the study, informing them that their responses would instantly be deleted without any consequences to their compensation. None of the participants chose to do so.

Besides the studies' consent form, both the shopping website and banking app contained additional privacy policies, informing participants about the data processing procedures. However, all relevant information was already stated clearly in the consent form, which participants had been shown at the beginning of the study. The privacy policies were only an additional resource to ensure participants feel comfortable.

When participants decided to participate in Study I (*Shopping*), participants were invited without mentioning a coupon, only advertising a study "to test an AI-assisted online shop." The shopping coupon they received via email was introduced after completing order one. Within the following shopping AI test and associated task description (for the second order), we informed them about improving their shopping AI score by making their composed "outfit as affordable as possible (e.g., use a coupon)," since the AI score calculation is based on the design and price-performance ratio of their final order. At no point did we promise participants that the coupon could be redeemed beyond the scope of the study or within a real commercial setting. As part of the debriefing, we provided a thorough explanation about the study's objectives and the nature of the coupon-related email.

Handling Email Addresses Participants' email addresses were forwarded directly to the mail provider Mailtrap, which handled the automatic delivery of emails and deleted email

addresses after a limited retention period of 7 days, in compliance with GDPR. Participants were informed about this in the survey and the data protection information on the website.

Handling Passwords Passwords participants created to register at the online shop in Study I were neither transmitted nor stored at any point. Instead (undisclosed to participants), any random string longer than six characters allowed participants to log in. We informed them about this procedure in the debriefing. It is possible that some participants entered passwords reused from real accounts. Although this did not pose a direct risk (since no data was transmitted) there is a small chance they saved these passwords to remember them during the study. However, since reused passwords are typically already memorized we consider this unlikely.

Lastly, our panel providers, TalkOnlinePanel and Cint, follow a self-commitment to the ICC/ESOMAR International Code on Market and Social Research [26].

8 Open Science

The artifacts including the data collected in all experiments, the codebooks for each open-ended question, the legitimate and malicious shopping websites and emails used in the *Shopping* use case, and the source code of both bankings apps used in the *Payment* use case, can be accessed through our permanent link (www.zenodo.org/records/15603931).

Acknowledgments This work was supported by the PhD School SecHuman – "Security for Humans in Cyberspace" by the federal state of NRW, Germany, and the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972.

References

[1] A. Bandura. Social Foundations of Thought and Action. *Englewood Cliffs*, pages 23–28, 1986.

[2] A. Bandura and N.E. Adams. Analysis of Self-efficacy Theory of Behavioral Change. *Cognitive Therapy and Research*, 1:287–310, 1977.

[3] Luka Bekavac, Simon Mayer, and Jannis Strecker. QR-Code Integrity by Design. In *ACM Conference Extended Abstracts on Human Factors in Computing Systems*, CHI EA '24, Honolulu, HI, USA, 2024. ACM.

[4] Kyle Blanker. Threat Spotlight: The Evolving Use of QR Codes in Phishing Attacks, October 2024. www.barracuda.com/qr-phish, as of June 12, 2025.

[5] Scanova Blog. QR Code Statistics 2024: Up-To-Date Numbers On Global QR Code Usage, February 2024. www.scanova.io/qr-statistic, as of June 12, 2025.

[6] Alina BÎZGĂ. Coupon Scams: What They Are, How They Happen, and How to Protect Yourself, July 2024. www.bitdefender.com/coupons, as of June 12, 2025.

[7] Canadian Centre for Cyber Security. Security Considerations for QR Codes, January 2024. www.cyber.gc.ca/security-considerations, as of June 12, 2025.

[8] Casey Inez Canfield, Baruch Fischhoff, and Alex Davis. Better Beware: Comparing Metacognition for Phishing and Legitimate Emails. *Metacognition and Learning*, 14(3):343–362, 2019.

[9] Dave Carberry. The Comeback Kid - The QR Code, February 2023. www.proofpoint.com/malicious-qr-code-detection, as of June 12, 2025.

[10] Xi Chen and Shun Cai. Self-Disclosure Under Social Networking Sites: A Risk-Utility Decision Model. In *International Conference on Electronic Commerce*, ICEC '12, pages 328–334, Singapore, Singapore, 2012. ACM.

[11] Denso Wave. Error Correction Feature, 2024. www.qrcode.com/errors, as of June 12, 2025.

[12] Denso Wave. QR Code Development Story, 2025. www.denso-wave.com/tech, as of June 12, 2025.

[13] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why Phishing Works. In *Conference on Human Factors in Computing Systems*, SIGCHI '06, pages 581–590, New York, NY, USA, 2006. ACM.

[14] DPA. Electric Car Owners Being Targeted by QR Code Scam When Recharging, 2024. www.yahoo.com/electric-car-owners-targeted, as of June 12, 2025.

[15] easyCharging.app. Watch Out! How to Avoid EV Charging Station Scams, February 2024. www.easycharging.app/avoid-ev-charging-scams, as of June 12, 2025.

[16] EMVCo. EMV QR Code Specification for Payment Systems – Merchant-Presented Mode, Version 1.1, 2017. www.github.io/emv-qrcode, as of June 12, 2025.

[17] EMVCo. EMV QR Codes, 2025. www.emvco.com/emv-technologies/qr-codes, as of June 12, 2025.

[18] European Central Bank. Single Euro Payments Area (SEPA), January 2023. www.ecb.europa.eu/sepa, as of June 12, 2025.

[19] European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2023, October 2023. www.enisa.europa.eu/threat-landscape, as of June 12, 2025.

[20] Sead Fadilpašić. QR Codes Are Being Used in Phishing Attacks Against US Institutions, August 2023. www.techradar.com/qr-codes-phishing-attacks-us-institutions, as of June 12, 2025.

[21] Federal Office for Information Security. State of Cybersecurity Concerning the Russian Assault on Ukraine, March 2022. www.bsi.de/ukraine-crisis, as of June 12, 2025.

[22] Nina Gerber, Alina Stöver, Justin Peschke, and Verena Zimmermann. Don't Accept All and Continue: Exploring Nudges for More Deliberate Interaction with Tracking Consent Notices. *Transactions on Computer-Human Interaction*, 31(1):1–36, November 2023.

[23] Nishant Goel, Ajay Sharma, and Sudhir Goswami. A Way to Secure a QR Code: SQR. In *2017 International Conference on Computing, Communication and Automation (ICCCA)*, pages 494–497, 2017.

[24] Ira Gosting. How The Pandemic Saved The QR Code From Extinction, March 2021. www.forbes.com/pandemic-saved-the-qr-code, as of June 12, 2025.

[25] ING. The Dangers of Scanning QR Codes From Email, 2024. www.ingwb.com/qr-codes, as of June 12, 2025.

[26] International Chamber of Commerce and ESOMAR. ICC/ESOMAR International Code on Market and Social Research, November 2016. www.iccwbo.org/iccesomar, as of June 12, 2025.

[27] International Organization for Standardization. ISO/IEC 18004:2015 – QR Code Bar Code Symbology Specification. Standard ISO/IEC 18004:2015, ISO, Geneva, Switzerland, 2015.

[28] IT Governance. What is Phishing? Attack Techniques & Prevention Tips, 2024. www.itgovernance.co.uk/phishing, as of June 12, 2025.

[29] ITonDemand. QR Code Scams Are on the Rise Again, November 2023. www.itondemand.com/qr-code-scams-rise-again, as of June 12, 2025.

[30] Daniel Jampen, Gürkan Gür, Thomas Sutter, and Bernhard Tellenbach. Don't Click: Towards an Effective Anti-phishing Training. A Comparative Literature Review. *Human-centric Computing and Information Sciences*, 10(1), August 2020.

[31] 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 *Workshop on Usable Security and Privacy*, USEC '24. ISOC, February 2024.

[32] Michael Kan. Don't Fall for It: Hackers Pounce on CrowdStrike Outage With Phishing Emails, July 2024. www.pcmag.com/crowdstrike, as of June 12, 2025.

[33] Keepnet. 2024 QR Code Phishing Trends: In-Depth Analysis of Rising Quishing Statistics, January 2024. www.keepnetlabs.com/qr-phishing-trends, as of June 12, 2025.

[34] 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 (Extended Version). www.leonalassak.com/qr-extended, as of June 12, 2025.

[35] Katharina Krombholz, Peter Frühwirt, Peter Kieseberg, Ioannis Kapsalis, Markus Huber, and Edgar Weippl. QR Code Security: A Survey of Attacks and Challenges for Usable Security. In *Human Aspects of Information Security, Privacy, and Trust*, HAS '14, pages 79–90, Heraklion, Crete, Greece, 2014. Springer.

[36] Katharina Krombholz, Peter Frühwirt, Thomas Rieder, Ioannis Kapsalis, Johanna Ullrich, and Edgar Weippl. QR Code Security – How Secure and Usable Apps Can Protect Users Against Malicious QR Codes. In *ARES*, pages 230–237, Toulouse, France, 2015. IEEE.

[37] Patrick Kühtreiber, Viktoriya Pak, and Delphine Reinhardt. Replication: The Effect of Differential Privacy Communication on German Users' Comprehension and Data Sharing Attitudes. In *Symposium on Usable Privacy and Security*, SOUPS '22, pages 117–134, Boston, MA, USA, August 2022. USENIX.

[38] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Cranor, and Jason Hong. Teaching Johnny Not to Fall for Phish. *ACM Trans. Internet Techn.*, 10(2):1–19, 2010.

[39] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. Phishing in Organizations: Findings from a Large-Scale and Long-Term Study. In *Symposium on Security and Privacy*, SP '22, pages 842–859, San Francisco, CA, USA, July 2022. IEEE.

[40] Yuan Li. A Multi-Level Model of Individual Information Privacy Beliefs. *Electronic Commerce Research and Application*, 13(1):32–44, 2014.

[41] Nina Marshall, Daniel Sturman, and Jaime C. Auton. Exploring the Evidence for Email Phishing Training: A Scoping Review. *Computers & Security*, 139, April 2024.

[42] Mattia Mossano, Oksana Kulyk, Benjamin Maximillian Berens, Elena Marie Häußler, and Melanie Volkamer. Influence of URL Formatting on Users' Phishing URL Detection. In *European Symposium on Usable Security*, EuroUSEC '23, pages 318–333, New York, NY, USA, 2023. ACM.

[43] National Cyber Security Centre (NSCS). QR Codes - What's the Real Risk?, 2024. www.ncsc.gov.uk/qr-codes-whats-real-risk, as of June 12, 2025.

[44] Anusha Nistane. Use Cases of PDF QR Codes for Various Sectors, August 2024. www.qrcodechimp.com/Use-of-PDF-QR-Codes, as of June 12, 2025.

[45] Gareth Norris, Alexandra Brookes, and David Dowell. The Psychology of Internet Fraud Victimisation: A Systematic Review. *Journal of Police and Criminal Psychology*, 34:231–245, 2019.

[46] Federal Bureau of Investigation (FBI). Cybercriminals Tampering with QR Codes to Steal Victim Funds, January 2022. www.ic3.gov/report, as of June 12, 2025.

[47] Ed Pearson, Cindy L. Bethel, Andrew F. Jarosz, and Mitchell E. Berman. "To Click or Not to Click Is the Question:" Fraudulent URL Identification Accuracy in a Community Sample. In *International Conference on Systems, Man, and Cybernetics*, SMC '17, pages 659–664, New York, NY, USA, 2017. IEEE.

[48] Justin Petelka, Yixin Zou, and Florian Schaub. Put Your Warning Where Your Link Is: Improving and Evaluating Email Phishing Warnings. In *Conference on Human Factors in Computing Systems*, CHI '19, pages 1–15, New York, NY, USA, 2019. ACM.

[49] Premium Parking. How to Stop Scammers from Skimming Parking Payments with Fake QR Codes, 2023. www.premiumparking.com/parking-payments-with-fake-qr-codes, as of June 12, 2025.

[50] Florian Quinkert, Martin Degeling, Jim Blythe, and Thorsten Holz. Be the Phisher – Understanding Users' Perception of Malicious Domains. In *ACM ASIACCS*, ASIA CCS '20, pages 263–276, Taipei, Taiwan, 2020. ACM.

[51] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana Von Landesberger, and Melanie Volkamer. An Investigation of Phishing Awareness and Education Over Time: When and How to Best Remind Users. In *Symposium on Usable Privacy and Security*, SOUPS '20, pages 259–284, Virtual Conference, August 2020. USENIX.

[52] Joshua Reynolds, Deepak Kumar, Zane Ma, Rohan Subramanian, Meishan Wu, Martin Shelton, Joshua Mason, Emily Stark, and Michael Bailey. Measuring Identity Confusion with Uniform Resource Locators. In *Conference on Human Factors in Computing Systems*, CHI '20, pages 1–12, Honolulu, HI, USA, 2020. ACM.

[53] Rio Grande. Don't Get Caught in a QR Code Scam, 2024. www.riograndecu.org/qr-code-scams, as of June 12, 2025.

[54] Santander. QR Code Scams: Protecting Your Money and Data, December 2023. www.santander.com/qr-code-scam, as of June 12, 2025.

[55] M. Angela Sasse, Jonas Hielscher, Jennifer Friedauer, and Annalina Buckmann. Rebooting IT Security Awareness – How Organisations Can Encourage and Sustain Secure Behaviours. In *European Symposium on Research in Computer Security*, ESORICS '22, pages 248–265, Copenhagen, Denmark, September 2022. Springer.

[56] Markus Schöps, Marco Gutfleisch, Eric Wolter, and M. Angela Sasse. Simulated Stress: A Case Study of the Effects of a Simulated Phishing Campaign on Employees' Perception, Stress and Self-Efficacy. In *USENIX Security Symposium*, USENIX '24, pages 4589–4606, Philadelphia, PA, USA, August 2024. USENIX.

[57] SecurePass. What is a QR Code – Its Working, Uses, Advantages, & Disadvantages, February 2024. www.thesecurepass.com/qr-codes, as of June 12, 2025.

[58] Jan Seeburger. No Cure for Curiosity: Linking Physical and Digital Urban Layers. In *Nordic Conference on Human-Computer Interaction: Making Sense Through Design*, NordiCHI '12, pages 247–256, New York, NY, USA, 2012. ACM.

[59] Filipo Sharevski, Amy Devine, Emma Pieroni, and Peter Jachim. Phishing with Malicious QR Codes. In *European Symposium on Usable Security*, EuroUSEC '22, pages 1–20, Karlsruhe, Germany, 2022. ACM.

[60] Filipo Sharevski, Mattia Mossano, Maxime Veit, Gunther Schiefer, and Melanie Volkamer. Exploring Phishing Threats through QR Codes in Naturalistic Settings. In *Symposium on Usable Security and Privacy*, USEC '24, San Diego, CA, USA, 2024. ISOC.

[61] Ashish Pratap Singh. Design a URL Shortener - System Design Interview, August 2024. www.algomaster.io/url-shortener, as of June 12, 2025.

[62] Teodor Sommestad and Henrik Karlzén. A Meta-Analysis of Field Experiments on Phishing Susceptibility. In *Symposium on Electronic Crime Research (eCrime)*, APWG '19, pages 1–14. IEEE, 2019.

[63] Ashley Stevenson. QR Code Login - How it Works and Implementation Process, November 2023. www.pingidentity.com/qr-code-login, as of June 12, 2025.

[64] George A. Thomopoulos, Dimitrios P. Lyras, and Christos A. Fidas. A Systematic Review and Research Challenges on Phishing Cyberattacks From an Electroencephalography and Gaze-Based Perspective. *Personal and Ubiquitous Computing*, 28(3):449–470, 2024.

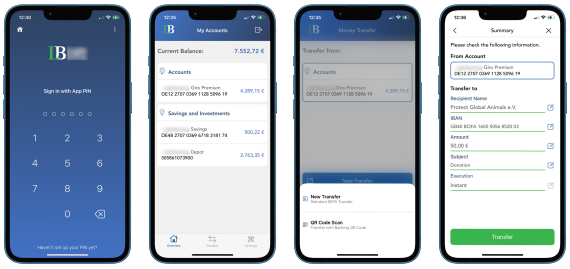
[65] UIUXTrend. Measuring and Interpreting System Usability Scale (SUS), November 2020. www.uiuxtrend.com/sus, as of June 12, 2025.

[66] U.S. Department of Homeland Security. The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research, 2012. www.dhs.gov/MenloPrinciples, as of June 12, 2025.

[67] Timothy Vidas, Emmanuel Owusu, Shuai Wang, Cheng Zeng, and Lorrie Cranor. QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks. In *International Conference on Financial Cryptography and Data Security*, FC '13, pages 52–69, Okinawa, Japan, 2013. Springer.

[68] Emma J. Williams and Danielle Polage. How Persuasive Is Phishing Email? The Role of Authentic Design, Influence and Current Events in Email Judgements. *Behaviour & Information Technology*, 38(2):184–197, 2019.

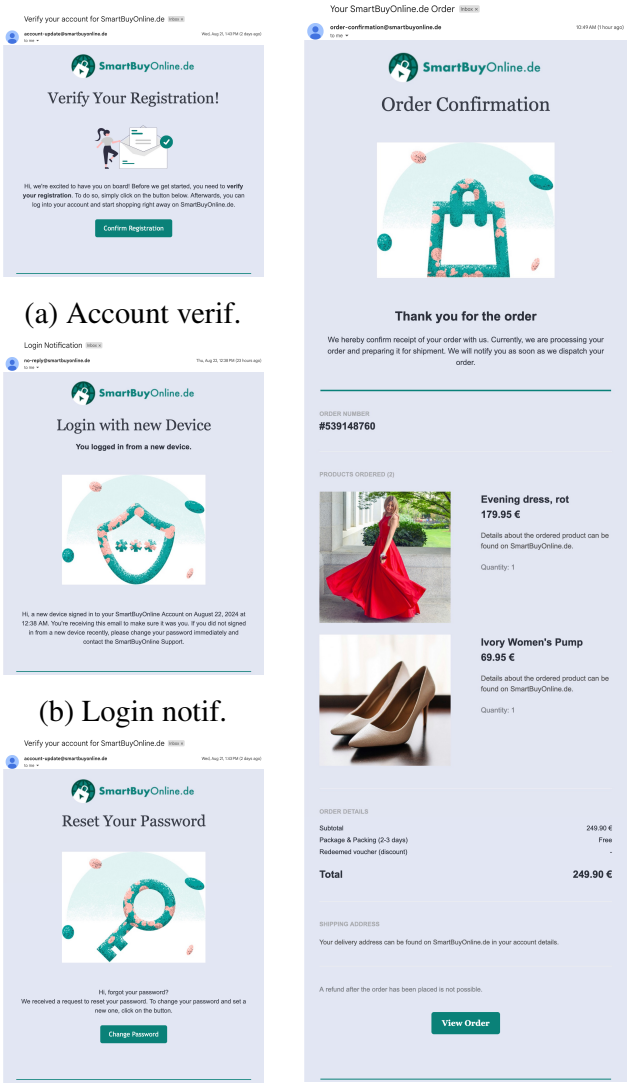
A Banking App Screenshots



(a) Login Screen. (b) Home Screen. (c) Transaction Menu. (d) Verification Screen.

Figure 6: Screenshots of banking app for *Payment* use case.

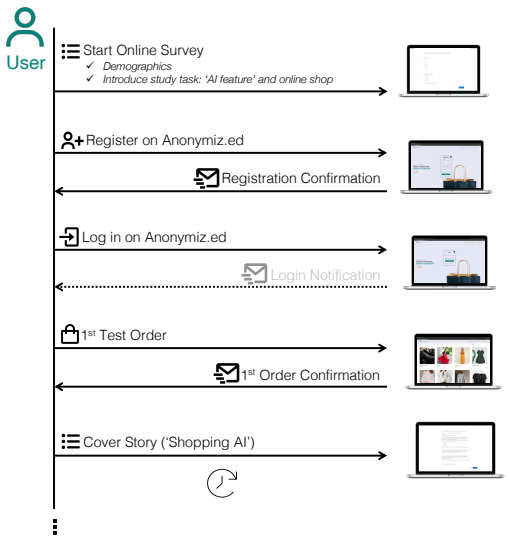
B Legitimate Emails From smartbuyonline.de



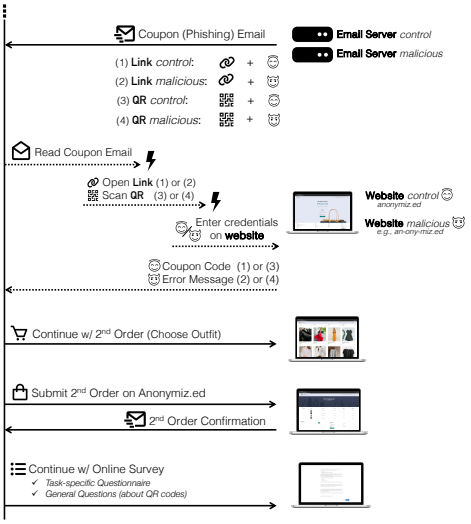
(a) Account verif. (b) Login notif. (c) Password reset. (d) Example order conf.

Figure 7: Emails sent from the *legitimate* SmartBuyOnline.de website to the participants.

C Overview Study Procedures.

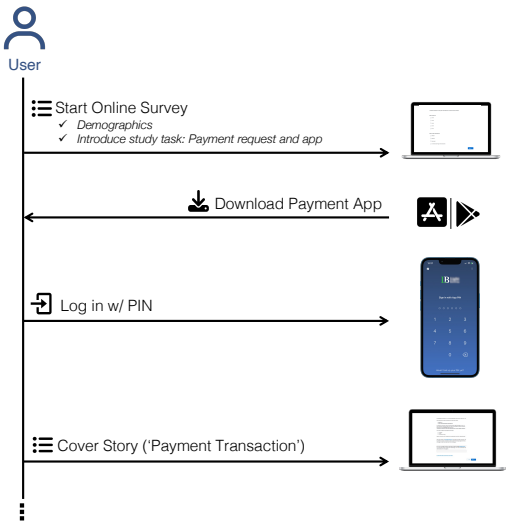


(a) 'Register & Familiarize with Online Shop'.

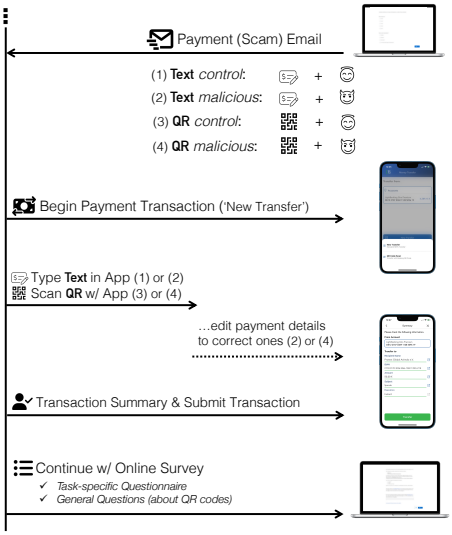


(b) 'Receive Coupon Email & Place Second Order'.

Figure 8: Overview of the *Shopping* study procedure.



(a) 'Download & Familiarize with App'.



(b) 'Perform Transaction'.

Figure 9: Overview of the *Payment* study procedure.

D Questionnaires

Study I: Online Shopping – Phishing

Demographics

D1 **How old are you?** Items: *18-29; 30-39; 40-49; 50-59; 60-74*

D2 **What is your gender?**

D3 **What is your highest level of education?**

D4 **Do you have practical experience in computer science, computer technology, or information technology (e. g., job or education)?**

Task-Specific Questions

S1 **How effortful did you perceive the registration and login process on SmartBuyOnline.de?** Items: *1: Not effortful – 5: Very effortful*

S2 **How effortful did you perceive the ordering process?**

S3 **How effortful did you perceive redeeming the coupon?**

S4 *[If used]* **Why did you use the coupon code from the email for your order?** *[Free response]*

S4' *[If not used]* **Why did you redeem the coupon code from the email but did not use it for your order?** *[Free response]*

S5 **We noticed you tried to redeem the coupon code. Why do you think it failed?** *[Free response]*

S6 **How trustworthy did you perceive the email with the coupon? (Email subject: 'Individual 50 € Coupon for SmartBuyOnline.de')** Items: *1: Not trustworthy – 5: Very trustworthy*

S7 **How trustworthy did you perceive the coupon website?**

S8 **Why didn't you enter your login credentials on the coupon website?** *[Free response]*

S9 **How trustworthy did you perceive the coupon website?**

S10 **Did you notice the email with the subject 'Individual 50 € Coupon for SmartBuyOnline.de'?** Items: *Yes; No*

S11 **Did you read the coupon email?** Items: *Yes; No*

S12 **Why did you open and read the coupon code email but did not *[click on the 'Redeem Coupon' button/scan the QR code/click on the link]*?** *[Free response]*

S13 **How trustworthy did you perceive the email with the coupon?**

General Questions: Online Shopping Behaviour

S14 **Do you use online shopping (e. g., Amazon)?**

S15 **Which of the following devices do you use for online shopping?** *[Multiple choice]* Items: *Smartphone; Tablet; Computer or laptop; Other devices: [Free text]; *Prefer not to answer.*

S16 **Do you access online shops through apps or through the internet browser?**

S17 **Have you ever used coupon codes to get a discount on your online purchases?** Items: *Yes; No; Prefer not to answer.*

Experiences with QR Codes

[Questions shared between both questionnaires are denoted with 'Q'.]

Q1 **In general, how effortful do you perceive using QR codes?**

Q2 **For which purposes have you used QR codes with your smartphone?**

Q3 **In general, how useful do you perceive QR codes?**

Q4 **Why haven't you used QR codes so far?** *[Free response]*

Q5 **How much do you agree with the following statement: QR codes may contain fake information.** Items: *1: Fully disagree – 5: Fully agree*

Q6 **How concerned are you that QR codes might contain fake information?** Items: *1: Not concerned – 5: Very concerned*

Q7 **Why do you believe that QR codes are (rather) unlikely to contain fake information?** *[Free response]*

Q8 **Why are you uncertain whether QR codes might contain fake information?** *[Free response]*

Q9 **Why do you believe that QR codes are (rather) likely to contain fake information?** *[Free response]*

Q10 **How or by what means can you potentially identify QR codes with malicious content?** *[Free response]*

Internet Fraud

Q11 **How concerned are you about falling victim to online fraud?** Items: *1: Not concerned – 5: Very concerned*

Q12 **Have you ever fallen victim to online fraud in general?**

Q13 **Have you ever fallen victim to online fraud through QR codes?**

SQ13 **Have you ever fallen victim to phishing?**

Confidence in Secure Behaviour on the Internet

Q14 **How confident are you to recognize an online fraud attempt?**

Q15 **How confident are you to recognize a phishing email?**

Q16 **How confident are you to recognize malicious QR codes?**

Knowledge and Misconceptions

Q17 **QR codes for opening websites are harder to fake than clickable links (URLs).** Items: *1: Fully disagree – 5: Fully agree; I don't know*

Q18 **QR codes are safe because they cannot be generated by scammers.**

Q19 **QR codes cannot be used for phishing (e. g., stealing user data like bank details or passwords).**

Q20 **QR codes are harmless.**

System Usability Scale

Please indicate how much you agree with each of the following statements.

SUS scale [65] Items: *1: Fully disagree – 5: Fully agree*

Privacy Disposition

Q31 **For each of the following statements, please indicate the extent to which you agree.**
[Items "Disposition to privacy" scale in the version of Yuan Li [40].]

Q32 **For each of the following statements, please indicate the extent to which you agree.**
[Items "Perceived Privacy Risk" scale of Chen and Cai [10].]

Study II: Online Payment – Financial Scam

Task-Specific Questions

B1 **How effortful did you find the login process in the app, particularly logging in using your app PIN?**

B2 **How effortful did you find the process of making the transfer?**

B3 **Describe the process of executing the transfer. Specifically, highlight any notable peculiarities that stood out to you.** *[free response]*

B4 **How secure did you find the wire transfer using the app?** Items: *1: Not secure – 5: Very secure*

B5 **How trustworthy (authentic) did you find the email in the scenario?** Items: *1: Not trustworthy – 5: Very trustworthy*

General Questions: Online Payment

B6 **Which of the following devices do you use for online banking?**

B7 **How many banking apps do you have installed on your smartphone?**

B8 **How frequently do you use an online banking app on your smartphone?**

B9 **How frequently do you use an online banking app on your tablet?**

B10 **How frequently do you log into your online banking account on a computer or laptop?**

B11 **Do you also use online banking for transfers?**

B12 **How frequently do you transfer money online?**

Experiences with QR codes *[see "Shopping" **Q1–Q10**]*

Internet Fraud *[see "Shopping" **Q11–Q13**]*

BQ13 **Have you ever mistakenly sent money to the wrong person?**

Confidence in Secure Internet *[see "Shopping" **Q14–Q16**]*

Knowledge and Misconceptions *[see "Shopping" **Q17–Q20**]*

Privacy Disposition *[see "Shopping" **Q31–Q32**]*