"To Pay or Not to Pay?": Understanding User Decision-Making and Influence of Nudges in UPI Apps

Abstract

In response to increasing social engineering attacks, Unified Payments Interface (UPI) apps have implemented a variety of *nudges* to deter users from responding to fraudulent payment requests. We conducted a scenario-based semi-structured interview study with 46 Indian participants who tested the impact of various user interface nudges to help them discern a mixture of fraudulent and non-fraudulent payment scenarios. Our study revealed a multi-stage decision-making process: participants relied on a digital literacy and security concern-based risk assessment, which is further influenced by their trust in the recipient as well as the perceived need of the financial transaction. Our results demonstrate that while most nudges help to combat fraudulent transactions, participants perceived "badges" (a nudge signaling the trustworthiness of the receiver) to be most effective in combating fraud. We conclude with concrete recommendations for current and future UPI developers.

CCS Concepts

• **Security and privacy → Usability in security and privacy**.

Keywords

Mobile Payment, Social Engineering, Mental Models, Nudges, United payments interface, UPI, Security, Scam, Nudges, India, Usability, Financial systems security

ACM Reference Format:

. 2026. "To Pay or Not to Pay?": Understanding User Decision-Making and Influence of Nudges in UPI Apps. In *ACM Asia Conference on Computer and Communications Security (ASIA CCS '26), June 1–5, 2026, Bangalore, India.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3779208.3785285

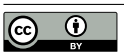
1 Introduction

Unified Payments Interface (UPI) is a widely popular mobile banking system in India for instant bank-to-bank transactions [67]. UPI is used daily by millions of users for purposes ranging from paying for groceries to sending money to friends or conducting business. UPI comprises a backend created by the Indian government, which is leveraged by a number of popular third-party apps. Since its introduction by the Reserve Bank of India in 2016, UPI has gained significant acceptance as a preferred mode of transaction. In 2018-2019, UPI accounted for 23% of the total volume of all Indian digital transactions, a figure that has surged to 55% in 2020-2021 [46] and further increased to 62% 2022-2023 [37]. UPI has achieved remarkable milestones, surpassing over 14 billion transactions in terms of volume and over ₹20.64 trillion (246 billion USD) in value in the month of July 2024 [14]. 605 banks [14] support UPI and more than 72 apps [13] are built on the UPI system. Some of the most popular UPI apps are PhonePe, GooglePay and Paytm. The number of monthly active users of UPI has escalated from approximately 30 million in March 2018 to over 491 million in June 2025 [27].

However, due to the widespread use of UPI apps, there has also been a notable surge in fraud associated with them, resulting in financial losses and privacy breaches of end users. These fraudulent activities often involve tricking users into sending money to attackers. The problem is compounded by the fact that UPI offers instantaneous, irreversible payment, effectively providing high usability but little or no consumer protection against fraud. In fiscal year 2023-24, there were 1.34 million recorded cases of UPI-based frauds—showing an increase from 95,000 in 2022-23, 84,000 in 2021-22 and 77,000 in 2020-21 [64] [26]. In fact, up to 73% of people using bank-to-bank transfers have been known to show concern about fraud and their trust in the system, and this number does not change significantly for seasoned users or young individuals [19].

Currently, most of the research related to attacks on UPI has focused on protocol-level security [55]. However, in contrast, a significant fraction of reported UPI fraud seems to have a strong user component, where fraudsters exploit loopholes in the mental models of users to trick them into financial harm, leading to loss of money from bank accounts [70]. A recent study discussed the gap in the guidelines released by authorities and the perceived information that influences users' mental model of UPI app usage [65]. In addition, we found that UPI apps offered by vendors like Paytm, PhonePe, or GooglePay often deploy security nudges in their interfaces to alert users with the intent to protect them from financial harm due to UPI fraud. However, there is no data-driven study to understand the attack strategies of common types of UPI fraud, the decision-making process of Indian users in the face of such fraud, or even the influence of interface nudges to combat fraud on UPI apps. Rapid adoption and retention of UPI in a country that has only a 27% financial literacy rate [6], making usage of UPI an exemplary case to study adoption of digital payment, risks, and digital assistance. This understanding can inform future work to make instant payment mobile systems more secure in India as well as other countries using similar mechanisms.

In order to understand users' decision-making process and the effectiveness of nudges, we first conducted a search of subreddits related to user experience of fraud. Using a thematic analysis, we were able to develop a taxonomy consisting of 4 popular UPI fraud strategies (Table 1). We then identified nudges deployed in real-world apps to help users identify fraud via a detailed study of the functionalities and interfaces of UPI apps. We leveraged these findings to build a UPI app simulator called UPI-Pay that emulates the real-world UPI experience. [1] The app was used to conduct semi-structured interviews with 46 participants who, like most



ASIA CCS '26, Bangalore, India

ACM ISBN 979-8-4007-2356-8/26/06
https://doi.org/10.1145/3779208.3785285

[1] Codebase of UPI-Pay is avialable here: https://github.com/spheresys/UPI-Simulator

consumers in India, were familiar with UPI as a tool in their day-to-day lives. Each of these participants were subjected to a set of five scenarios randomly picked from ten curated scenarios across different fraud types (Table 1) and nudge combinations.Based on the data gathered by interactions between the UPI-Pay app and our participants, we further evaluated the impact of nudges in alerting users to a fraudulent scenario. Specifically, we answer two research questions in this study to understand the users' mental model and nudge design preferences to enhance user experience.

RQ1 - *What is the users' decision-making process during a UPI transaction?*

Our study uncovered that users employ a security risk-assessment mechanism when they make a UPI transaction. The assessment uses three criteria: validity of the transaction request, necessity of providing the requested information, and mismatched context. This assessment is found to be heavily influenced by their digital literacy. However, the results of risk assessment for a UPI transaction are often overridden by users' trust in the recipient or their need to do the financial transaction. Our work takes a first step towards identifying the decision-making process of UPI users during online transactions. We considered both fraudulent as well as non-fraudulent transactions in our study.

The users' response to UPI-Pay when subjected to a random combination of fraudulent and non-fraudulent scenarios in our study showed that they were substantially less likely to fall for fraud when there were nudges present in the interface, making correct decisions 82.58% of the time (i.e., allowing non-fraudulent transactions while blocking fraudulent transactions) as compared to 65.38% of the time for scenarios with no nudge. Having learned that nudges positively impact users' decisions while using UPI apps, we further studied their preferred nudge designs and their influence on UPI usage experience.

RQ2 - *What are the user preferences to enhance the design of UPI apps to improve protection against fraud?*

On analysis of qualitative data obtained during the semi-structured interview we found that "badges" (a nudge used to signify how much trust users should put in the recipient) was the most preferred nudge among participants for combating fraud. This was followed by "screen-blocking notification" that forced users to reconsider proceeding with a transaction. Participants' post-interaction (with UPI Pay) reflections also point to future directions for protecting users against UPI fraud. This includes system-provided signals to establish trust in the recipient, deploying contextual nudges, and improving digital literacy.

Our work lays the foundation for understanding how users decide to perform a UPI transaction and how nudges can help users in identifying fraudulent transactions. Comparative study of the effectiveness of nudges is a valuable future work to quantify the impact of different nudge designs and prescribe precise modifications. Our work of understanding user preferences and decision-making process is especially crucial as instant bank transfers are becoming more common in many countries e.g., FPS (UK), DuitNow (Malaysia), and NPP (Australia) [21] and will potentially become more ubiquitous and prevalent for completing a large variety of everyday purchases. In summary, we take a step to identify how to assist users in combating fraudulent transactions and encourage designers and researchers to further explore and develop such mechanisms to better protect end users.

2 Background and Related Work

We first introduce UPI and its characteristics followed by our data-driven taxonomy of popular UPI frauds.

2.1 Background

Unified Payments Interface (UPI): UPI [14] is an instant mobile banking system developed in India and launched in 2016. UPI provides an API of an Indian government-regulated back end for instantaneous bank-to-bank money transfers between Indian bank accounts. The only prerequisite for using UPI is to have a valid bank account in the Indian banking system, linked to a mobile number. The current UPI version (UPI 2.0) addresses the security issues identified in UPI 1.0 by Kumar et al. [55]. UPI 2.0 also contains security features like signed QR for payments and invoice generation to improve trust and authenticity of the system [32]. Based on the UPI protocol a number of vendors created popular UPI apps (e.g., Paytm [10], Google Pay [1], and PhonePe [11]) to enable seamless, instantaneous financial transactions between bank accounts. The phrase "UPI" is often used to refer to these payment apps based on the UPI system, not just the UPI protocol. Thus, going ahead, we also use UPI to refer to these apps. As of 2024, UPI has over 350 million active users and 340 million QR codes at merchant locations [20, 41, 54, 73, 77]. Currently, UPI involves 605 banks [14] and more than 72 UPI apps [13]. Starting in 2022, UPI has also been adopted beyond India, in France, Australia, Singapore, the UAE, Sri Lanka, Nepal, and Bhutan [83].

UPI has clocked over 19.4 billion transactions in the month of July 2025, in terms of volume and ₹25,08,4980 million in terms of value [14]. Millions of users use UPI because of its adaptability, smooth integration with other platforms, and government support, which have all contributed significantly to its exponential expansion. In terms of the number of users who have adopted it, the volume of transactions, and the number of transactions executed by an eclectic population, it is regarded as one of the most successful payment systems in the world.

In a population of over 1.42 billion [53] India observed that only the top 1% of the country continued to control 53% of the country's wealth, signifying a lack of convergence and accessibility [75]. This led the Reserve Bank of India (RBI) [72] to establish its vision for payments in 2018: Coverage, Convenience, Confidence (integrity and security), Cost, and Convergence. The government of India mandated Aadhaar [28] as a digital identity for every citizen of India in 2010 and launched a financial inclusion program Prime Minister's Jan-Dhan Yojana to promote transparency and inclusion for all Indians in 2014. Simultaneously, it was observed that mobile penetration in the country had surged in 2016 [76].

By mapping these patterns together, NPCI [2] envisioned Unified Payments Interface (UPI). UPI is a centrally standardized system that powers multiple bank accounts into a single mobile application (of any participating bank). It is an instant and real-time mobile

[2]National Payments Corporation of India (NPCI) is an organization that operates retail transaction and settlement systems

payment system that enables peer-to-peer and peer-to-merchant transactions between banks. It was a futuristic solution that had the power to converge (the 5th C of India's vision payments) all individuals and businesses under one convenient protocol with the sole need of having a bank account. It is regulated by the RBI, which is the regulatory body of the Indian banking system.

Comparison between UPI and other payment apps: There are other widely used online mobile payment applications, such as PayPal [9], Venmo [15], and Zelle [18] with similar basic functionality—financial transactions. In fact, there are other less-popular but similar apps, e.g., FPS, DuitNow, and NPP in the United Kingdom, Malaysia, and Australia, respectively [21]. However, there are some key differences between UPI and the existing popular payment apps, which necessitates this study. We discuss the difference across four factors—type of usage, the time for money transfer, buyer protection policy and volume of frauds committed.

Venmo (85.1 million active users in 2023) and Zelle (120 million active users in 2023) are often used by students for food, and transportation while PayPal (220 million active users in 2023) is commonly used for transactions between individuals and businesses [29, 71, 79, 86, 87]. In contrast, UPI stands out as a versatile option used by people all across India, ranging from paying for groceries and giving money to associates/family to conducting large value business transactions (e.g., buying gold). Thus, the potential for fraud in UPI is significantly greater due to the varied context of use. Furthermore, UPI enables instant money transfer (like Zelle). In comparison, PayPal and Venmo transactions may take from 30 minutes to 5 days [5, 16] to settle payments, and users can revert payments within this time. In addition, UPI provides lesser consumer protection—UPI payments are irreversible and the victims need to contact law enforcement and banks to request a refund. Whereas, when requested via respective apps in 2021, the refund success rates are respectively 47.4%, 14.3%, and 0.9% for PayPal, Venmo, and Zelle [2].

Zelle and UPI are similar in terms of money transfer time and weak refund rate, while they widely differ in transaction volume and likelihood of fraud. The likelihood of fraud in Venmo and Zelle is approximately 4% [8]. Conversely, recent studies reveal that in India, nearly 50% [3] of financial fraud cases are linked to UPI. Thus, UPI provides a small margin of error for its wide Indian user base and has a greater chance for financial harm due to fraud compared to other platforms.

UPI frauds: The popularity of UPI, combined with instantaneous money transfer and lower consumer protection, resulted in an ever-growing trend of UPI frauds. Over 1.34 million fraud cases were registered in 2023-24, 95,000 cases in 2022-23, an increase from 77,000 cases in 2020-21 [34, 39, 64]. Despite the growing rate of frauds, the different types of UPI frauds and how do Indian users navigate through them in not clear–we fill this gap.

2.1.1 Creating a Taxonomy of Popular UPI Frauds. When we started, we noted that there is no taxonomy of popular UPI fraud strategies. We leveraged crowdsourced data of Indian users' experiences with UPI frauds to identify popular strategies for UPI frauds.

Collecting data on UPI fraud experiences: We collected potential webpages stating user experiences with UPI frauds using web search in subreddits (r/India, r/IndiaSpeaks, r/cybersecurity) and Google using keywords like "UPI Fraud Types", "UPI Frauds", and "Top UPI Frauds" (see appendix F for full list). In total, we collected 793 webpages. However, not all of them were related to user experiences of UPI frauds. A researcher manually examined these webpages and identified 60 webpages that stated personal user experiences with UPI frauds or scams that leveraged user interaction (i.e., social engineering) and UPI features (e.g., fooling users into sending money to scammer' accounts).

UPI frauds	Description
Request Money Fraud [12]	Impersonate a representative of a reputed company (e.g., via calling the user) and request money from the users by offering them lucrative fake offers
Forged QR [7]	UPI transactions can be done by a user scanning QR codes which contain both embedded UPI ID and transaction value. In this attack, attackers distract users and make them not notice the value embedded in the attacker-provided QR code, so that it's more than the actual value the person was expected to pay.
Fake Payment screen [17]	Attackers trick users into believing that a transaction would credit money into the user's account, but on completion, the user's account will end up being debited that amount.
Deceptive UPI Handles [43]	Attackers create deceptive UPI handles based on famous and trusted organizations (e.g., Facebook, Amazon) to scam users and receive payment.

Table 1: Four types of UPI frauds exploiting UPI users' decision (citations show webpages with specific user experiences)

Thematic analysis of experiences with UPI frauds: We used a thematic coding-based approach from user experiences to create our fraud taxonomy [44]. Two researchers independently reviewed fraud descriptions extracted from the web pages in a randomized order. While reviewing, each of them continually compared new story descriptions, grouping together attacks with similar descriptions and attack strategies (thus identifying themes). Subsequently, the researchers convened, cross-referenced the groups of stories they created (while identifying similar groups of stories), and collaboratively finalized the categorization. This approach led to the identification of four specific UPI fraud strategies, each of which exploits users' decision-making processes. Due to the collaborative nature of analysis, we did not compute inter-rater agreement.

Taxonomy of UPI frauds: We ultimately identified 4 types of UPI frauds (Table 1) using our thematic analysis. These categories also align with Stanford's taxonomy of financial frauds [4]. In each case, the fraud begins with the attackers contacting the end user (e.g., via phone or text) and then deceiving them into willingly initiating transactions to send money to the attackers, effectively influencing user decisions. We will leverage fraudulent scenarios constructed from this taxonomy to uncover UPI users' decision-making process.

2.2 Related Work

We will now review related work on mobile payment app adoption and fraud on these apps.

User adoption of payment apps: Prior work has explored the user adoption process of mobile banking systems in different populations. Hanif et al. [47] found that adoption of mobile banking in older (aged 55+) UK users depends on performance expectancy and perceived security risk. Kuriakose et al. [56] specifically discussed the user adoption intention of UPI and developed a new model for identifying the factors influencing the adoption of UPI. Our study is built on these efforts since the wide adoption of UPI resulted in fraud and necessitates our study on uncovering the decision-making process of UPI users when doing both fraudulent and non-fraudulent transactions.

Frauds leveraging social engineering: There has been extensive research on how social engineering techniques (e.g., phishing) are used by scammers to manipulate performing actions or divulge confidential information [22]. Earlier work explored why people fall for phishing: Technical Phishing Prevention, Human-Centered Phishing Prevention [82], security preferences of users, the steps taken to ensure safety [68] and phishing susceptibility [84] helps to understand the reasons and ideal route for mitigation. Hashmi et al. presents security mechanisms motivated by loan app scams in Pakistan that specifically target low socioeconomic users who are particularly vulnerable [49]. However, no earlier work explored the decision-making process of Indian UPI users, which led to financial harm. In our study, we also draw from earlier work [45], e.g., to identify nudges in UPI apps that might have influenced this decision-making process. Our results align with existing research on phishing attacks and banking frauds, emphasizing digital literacy, awareness, and need as fundamental themes and frameworks [31, 50]. However, they did not uncover how these factors interact during *decision-making process* of financial transactions. Furthermore, an analysis of the effect of nudges and recommendations was not done. We address this gap.

Attacks on UPI apps: Previous work focused on the drawbacks of UPI protocol [55]. UPI 2.0 already addresses these issues. However, the rise of attacks on UPI users is often tied to faulty decision-making processes of users (e.g., as identified in our attack taxonomy) rather than issues in the UPI protocol. Consequently, we identify that different UPI apps today deploy different security nudges (Section 3.2). However, the impact of such nudges on the UPI users' decision process (and their effectiveness in stopping fraud) is not quite clear. Understanding the efficacy of these nudges and providing data-driven suggestions is of utmost importance to protect UPI users against fraud. In this work, we answer this call.

User perception of UPI apps: A recent study conducted a survey [65] to gauge how users perceive UPI apps and what is the gap between the advice shared by the authorities and the experience of its users. The research underscored 10 concerns: 1) Participants express distrust towards UPI apps and prefer to use UPI services from their banks, 2) Users conflate scams with UPI platforms, 3) Cybercrime complaints are mostly unreliable and unhelpful, 4) Participants worry about security risks of leaving devices at repair shops, 5) Participants worry about losing their device but are familiar with follow-up, 6) Auto debit feature in UPI exacerbates safety concerns, 7) Participants follow default security settings on UPI apps, unaware of other safety settings, 8) Biometric authentication for UPI feels more secure than other authentication methods, 9) Participants prefer PIN-based transactions over "UPI Lite" feature for security and control reasons, 10) Participants prefer PIN authentication over pattern locks for safety reasons. These concerns can be categorized into 4 disjoint buckets: 1) Lack of trust on the platform 2) Lack of trust on people 3) Lack of digital literacy 4) Authentication/ security preferences. The concerns with UPI were followed by a detailed display of the advice by authorised bodies concerning UPI showcased the perception of UPI. However, it does not closely analyse the mental model and decision-making process of UPI users during a transaction. In our study we will focus on understanding the decision-making process of UPI users and the impact of user interface nudges in preventing fraud.

3 Survey of UPI App Functionalities

Note that the UPI API was provided by the Indian government's regulatory bodies, but a number of vendors developed UPI apps based on this API. These apps are different in terms of functionality and interfaces. Thus, in order to uncover the decision-making process, aside from fraud taxonomy, we needed to identify the functionalities and interfaces provided by popular UPI apps and leveraged by fraudsters. We focus on the most popular UPI apps in India— PhonePe, Google Pay, and Paytm that flourish with a market share of 46.3%, 36.4%, and 10.2% respectively [25]. To identify common functionalities and interface elements of these UPI apps, we performed a survey of popular UPI app functionalities by two researchers who are also UPI users (in line with prior work [35]).

Method: Two researchers independently installed a fresh copy of these three apps on their phones and followed a prescribed set of actions (in Appendix A) while writing down notes about the basic functionalities, the steps in a transaction, differences, security features, and nudges implemented by the interface design [45, 84]). Note that both researchers had a registered UPI ID (and an associated mobile number). Finally, the researchers exchanged their notes and independently identified the list of functionalities, interface elements, and nudges (i.e., alert screens, differently colored or formatted text) mentioned in at least one of the notes. Finally, they met, combined their lists, and created a final set of basic functionalities, major interface elements, and nudges.

3.1 Key Functionalities and Interface Elements of UPI

In this section, we present the basic functionalities of UPI apps (in the context of financial transactions) as identified by our study of UPI App functionalities and the major interface elements commonly used across the apps.

Download and signup process: All surveyed apps are available on Google Play Store and Apple App Store. To start using UPI, the user needs to register using a phone number associated with the corresponding bank account. The user needs to set a PIN while signing up which will be used to send money. However, PIN is not required for receiving money.

Basic functionalities of UPI apps: We identified six basic functionalities across the three UPI apps–Send money, Request money, Scan QR code and Pay, Show transaction history, Show user profile, Show/Choose bank account for transaction. We further noted

Interface components	Description
Home page	First page when the UPI apps are opened. It enables Send Money via QR code and contact number, Request Money and, opening the Profile.
Get my balance page	Accessed by clicking on the user logo on the top of the home page. It allows the user to check their bank balance by entering their UPI PIN.
Payee information and transaction	Accessed by entering the name of the payee in the search bar on the home page. This page shows the transaction and chat history with that individual/business.
Transaction views	Shown in the last step of any transaction. Consists of Bank account selection view, UPI Pin Entering view, and Transaction completion status view.
Payment request view	Triggered by the requester externally via the Request Money feature and appears on the payer's home page.

Table 2: Five major interface components present in UPI apps and noted during our survey of UPI apps that enable six basic functionalities

their description (Table 9 of Appendix G). The functionalities are often similar across apps with minor variations in name, button appearance, and exit options.

Major interface components: We further identified five major components in the user interface of the three UPI apps during our study. These components enable the six basic functionalities, and their design potentially impacts user decision-making. These components are shown in Table 2. These functionalities and components provide us with a unified specification for popular UPI apps that influence users' decision-making process.

Help and support: The popular UPI apps, including Google Pay, PhonePe, and Paytm, also provide Help and Support features. However, we noted that they are often geared towards helping users when they face problems like failed payments. This help generally does not provide a point of support when users are defrauded and lose money.

3.2 Identifying Nudges

Nudges are design interventions that subtly guide individuals towards a desired course of action. Leonard et al. [59] describe nudges as "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives". These nudges are first defenses against phishing and social engineering attacks [30, 58, 66, 80, 88]. In line with that finding, we expect the nudges in UPI apps to potentially impact the users' decision-making process when they are attacked by fraudsters.

Leveraging nudge taxonomy of Franz et al. [45]: We leveraged the taxonomy of different user-oriented phishing interventions by Franz et al. [45]. These interventions are education, training, awareness campaigns, and design strategies (details in Table 8 of Appendix G). Specifically, two researchers examined multiple UPI apps and their UPI interfaces, identifying the design elements they deemed as nudges. We ultimately identified four different nudges in various UPI apps (Table 4) by aligning the taxonomy of user-oriented phishing interventions (Table 3) with the identified design elements. We considered these to assess the decision-making process of users against different fraudulent scenarios.

Nudge	Category of user oriented design interventions	
	Awareness - raising	Design
Badge	Passive Warning	Color Code, Visual Element
Amount will be deducted	Passive Warning	Color Code, Highlighting, Passive Warning
View-once notification	Passive Warning	Highlighting
Screen blocking notification	Interactive Warning	Highlighting, Color Code

Table 3: Alignment of four *nudges* found in UPI apps during our study with Franz et al.'s framework

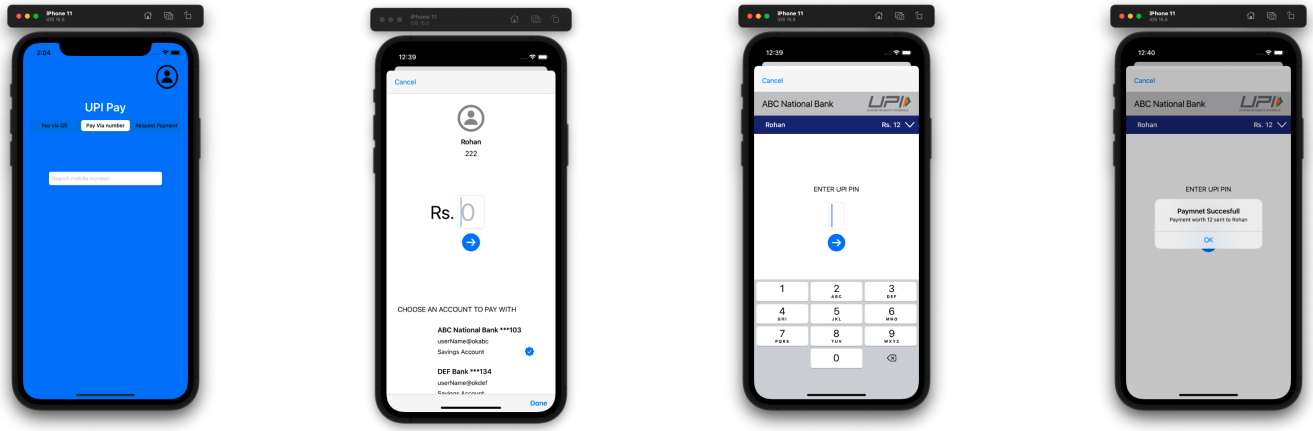
Nudge Name	Description	Example Figures (Appendix H)
Badge	Shows if the transaction receiver is trusted	Figure 2b, Figure 2c, Figure 2d
Amount will be deducted	Gathers the user's attention to the transaction, helps in cases of lack of attention and/or digital literacy	Figure 2a
View-once notification	Nudge the user to recheck transaction details	Figure 2f
Screen blocking notification	Forces the user to recheck transaction details as it freezes the screen and forcefully gathers the user's attention to it	Figure 2e

Table 4: The list of four key nudges found in UPI apps

4 Study Methodology

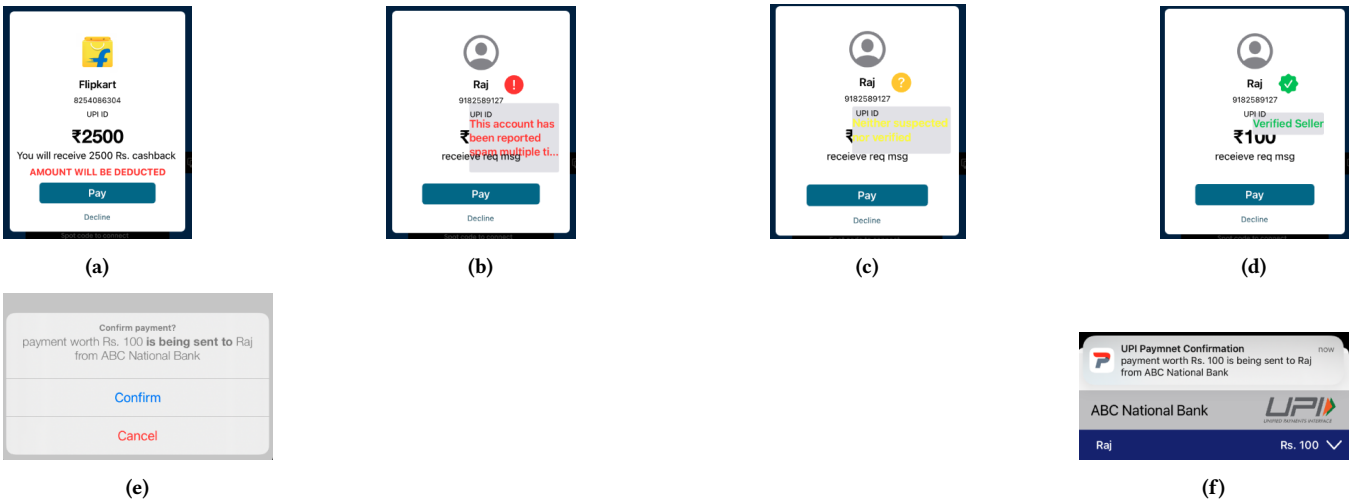
In this work, we aim to uncover UPI users' decision-making process while completing financial transactions (both fraudulent and non-fraudulent) while they are subjected to the nudges deployed in real-world UPI apps. Thus, we performed a semi-structured interview study using a novel UPI-simulator.

Study components: Our study design comprised two key components: First, we created a desktop UPI simulator called UPI-Pay (grounded in the functionalities, interface components, and nudges of Section 3). Second, we performed a semi-structured interview for a set of participants (chosen via a pre-interview survey) to interact with UPI-Pay while facing randomly chosen fraudulent (grounded in the fraud taxonomy of Section 2.1) and non-fraudulent transaction scenarios.



(a) (b) (c) (d)

Figure 1: Steps followed by a user while paying via contact number on UPI-Pay: (a) Search receiver (b) Enter transaction amount (c) Enter pin number (d) See completion status



(a) (b) (c) (d) (e) (f)

Figure 2: Different *nudge* designs incorporated in the app (a) Amount to be deducted (b) Red badge (signifying reported as malicious) (c) Yellow badge (signifying neither suspected nor verified) (d) Green badge (signifying verified trusted users) (e) Screen blocking notification and (f) View-once notification

Rationale for using a simulator: Since UPI apps are sensitive software containing users' financial information, we refrained from instrumenting real UPI apps in users' phones or asking users to interact with their own UPI apps to remain ethical (since it might cause financial harm to users). Our pre-app development pilot also indicated that users are reluctant to install experimental UPI apps on their phones. Rather, we explored an ethical alternative approach to present users with realistic UPI transaction scenarios in a desktop app. To fetch the most realistic data, we crafted the UPI-Pay app and transaction scenarios using a real data-driven interface and fraud scenarios (the form factor of the UPI-Pay app is exactly similar to a mobile device). Furthermore, the study design was assured to be ethical beyond confusion by deploying the app on the researcher's desktop, such that no personal app usage data was shared by the user. We were concerned that our desktop app might have some impact on how users would use and perceive it compared to the mobile-based apps. To that end, previous work identified that mobile usage provides a higher cognitive load to users, which may lead to impulsive behavior and less considered security-sensitive decisions [38, 52]. Thus, the results in this paper provide a lower bound of susceptibility of users towards UPI fraud–in a mobile environment, users might perform worse (perhaps due to haste) while facing fraudulent transactions.

4.1 Designing UPI-Pay: A UPI App Simulator

Basic design: We created the UPI-Pay app using the mobile simulator provided by XCode[23] and incorporated all the functionalities and interface elements uncovered by a survey study of three popular UPI apps (Section 3). We noted that the interface of the three most popular UPI apps is the same across iOS and Android, the two major OS in the mobile industry [24], making it familiar for users of both platforms. The simulator was installed on the machines of three researchers who conducted the interviews, whereas participants joined the interview using the Zoom app (in order not to require them to travel to our lab) and did not need to install our simulator on their machines. Participants interacted with our simulated UPI app via Zoom's remote control feature [89]. A pilot study on two users who inspected UPI-Pay with a researcher verified that the UPI-Pay interface was understandable and unambiguous. In the pilot studies, the participants took around 5 minutes to get familiar with UPI-Pay and use its functionalities. We show the working of the UPI-Pay simulator app where participants perform "Pay via contact no." in Appendix B. The code base of UPI-Pay is available here: https://github.com/spheresys/UPI-Simulator.

Incorporating nudges in UPI-Pay: To test the efficacy of different nudges for protecting UPI users against fraud, we implemented the nudges identified in Table 4. For the "badges" nudge (which emulates the verified symbols provided by some of the UPI apps like GooglePay) we added three variants with different colors–red, yellow, and green. The colors are chosen considering the effects these colors have on the human mind [36, 57]. Appendix H presents screenshots of the nudge interfaces implemented in UPI-Pay.

In our study, when we asked the users to do a transaction, we did not show all nudges in a single transaction, e.g., "screen blocking notifications" and "view-once notifications" present the same information and are not shown in a single transaction. Specifically, for each UPI-Pay transaction in our study, we randomly selected one of 12 possible conditions: 11 subsets combining different configurations of three nudges– "badges" (present or absent), "amount will be deducted" (present or absent), "Notification type" (screen-blocking, view-once or absent) and one control condition with no nudges.

4.2 Study Protocol

Our study protocol comprised a pre-interview survey and a semi-structured interview conducted via Zoom.

Pre-Interview survey: First, we shared a recruitment form with details about the study and requested interested candidates to fill out a pre-interview survey (Appendix C) to record their demographic details and past experience with using UPI.

Semi-structured think-aloud interview: The selected participants were invited to a Zoom session where the interviewer read the consent form to obtain verbal consent. Then the interview was conducted in three phases. In the first phase, the interviewer **introduced** UPI-Pay (installed on the interviewer's computer). Participants interacted with UPI-Pay installed on the interviewer's computer via Zoom's remote control feature. The participant conducted an example transaction in UPI-Pay to familiarize themselves (with the interviewer helping them if needed). In the second phase, we did a **think aloud transaction simulation** where each participant is shown 5 transaction scenarios at random (out of 10 real-data inspired scenarios—five fraudulent and five non-fraudulent) and is requested to decide whether to do the transaction. Note that UPI-Pay randomly chose subsets of nudges to show in each scenario. In the third phase, we did a **debriefing, mitigation, and feedback** where the interviewer discussed the user's decisions and corrected any mistakes. Then the participants shared their experiences with UPI frauds and rated nudge designs based on perceived efficacy (on a scale of 10). Finally, the interviewer transfers the gift card. We recorded the interview with user consent (audio recording, screen recording, and UPI-Pay execution logs). The interview instrument is in Appendix D.

4.3 Recruitment

We circulated an online recruitment form (and pre-interview survey) between May 2022 and December 2022 via mailing lists of university students. We also encouraged participation from their relatives to access a diverse group. We additionally distributed paper forms (and a survey) in cafes within a university campus and in two large Indian metro cities. We chose participants who were at least 18 years old, proficient in English or Hindi, and had used at least one UPI app to some extent–they were contacted via email and took 50 to 60 minutes to complete the interview. Each participant was compensated with ₹300 (3.6 USD/hr) with anAmazon Pay gift card which is around 1.5 times the median hourly salary of an Indian worker (for a 40 hour work week) [74].

4.4 Ethics Considerations and Compliance with the Open Science Policy

Our study design was approved by the IRB of one of the authors, and we went through multiple iterations to modify our protocol for not collecting any sensitive data during the study. The UPI-Pay simulator app ran on the interviewer's desktop to ensure that no personal data or money of the participant was involved. We maintained complete transparency with the participants, and the screen and audio recording was collected only after informed consent. We removed any personal identifiers from the data to maintain privacy. To comply with the open science policy, our study instruments are in Appendix A, C, and D. We will further share the codebase of UPI-Pay as well as quotes in our theme hierarchy upon publication.

4.5 Limitations

Our decision to use a desktop-based UPI app simulator instead of an app was due to ethical reasons such as security and privacy concerns among users and to facilitate scalability, explained in our rationale of using the UPI-Pay desktop app (Section 4). We scaled our desktop view to the size of a phone to simulate a mobile experience. Moreover, in the mobile environment, users are prone to less consider security-sensitive decisions [38, 52], thus, our participants likely thought more carefully than they would do for a mobile app, making the results on their susceptibility to fraud a lower bound. We attempted to recruit a diverse sample representative of the Indian population, however, our participant pool has a bias towards young Indians working in or having knowledge about IT or related fields. We note that these users are the natural users of UPI and their

Age	18 - 24	19
	25 - 34	11
	>34	16
Gender	Male	28
	Female	18
IT Jobs/education	Yes	35
	No	11
Education	College graduate or higher	38
	Did not complete college	8
Years of UPI use	<1 year	8
	1 - 2 years	12
	>2 years	26

Table 5: Demographics of 46 participants from our study.

potential familiarity makes the concerns uncovered in this study a lower bound on concerns from real-world users. We recruited participants for this study until we achieved thematic saturation (Section 4.6). We acknowledge that the cultural background, past experiences, age group, and social circles of our participants across India could have an impact on their decision-making process and usability preferences that we have not captured as part of this study. Our study is most relevant to the young and educated strata of India. Our think-aloud protocol allowed us to uncover users' key decision-making process [51]. Due to the qualitative nature of the study, it is possible that our data may be subject to bias such as desirability bias and chilling effect. We further randomized the scenarios presented to users to avoid order bias.

4.6 Participants

We first conducted two pilot studies to test and improve our UPI simulator as well as study protocol.

Ensuring thematic saturation: In our qualitative analysis strategy (Section 5), we first conducted 40 semi-structured interviews with Indian UPI users and performed qualitative analysis to uncover themes in decision-making process. Then we performed 4 more interviews and enhanced the themes. Finally, we conducted 2 more interviews and observed that no new themes emerged, identifying thematic saturation.

Demographics: We present the demographics of the final 46 participants in Table 5. 39.13% of our participants identified as female, consistent with the proportion of female users utilizing UPI [69]. Majority (35 participants) self-reported having IT Jobs/education and 8 participants did not complete college. The age distribution of our participants was as follows: 41.30% were aged 18–24, 23.91% were aged 25–34, and 34.78% were above 34 years old, indicating a diverse sample across young and middle-aged adults.

5 Data Analysis

Language translation: Some of the interview transcripts are in Hindi which we translated into English using Maestra [61]. Then a researcher proficient in both Hindi and English checked the translation, fixed errors, and created the final transcripts. Hindi text (where applicable) corresponding to English text used in the paper are in Table 7 of Appendix E.

Qualitative analysis: Two researchers first independently read through the transcripts, flagging all quotes from the transcripts that were potentially explanatory of decision-making process during UPI transactions by the participants. A total of 1,041 quotes from the 46 interviews were identified by at least one researcher as potentially explanatory. Next, one researcher selected 10% random quotes and created an initial codebook. Then, two researchers individually open-coded all the quotes, augmenting the codebook if necessary. Finally, they met to discuss specific disagreements and assign a final code to each quote, resulting in 30 codes. The inter-rater agreement (Cohen's Kappa) was more than 0.65, signifying substantial agreement [63]. Three researchers then collaboratively analyzed those 30 codes using an *affinity diagramming* process, where they together looked into the set of quotes with each code, not only the code itself [48]. They collaboratively created hierarchical themes using an iterative consensus-building technique to investigate the decision-making process (RQ1). We iteratively added more interviews and repeated the above process to check if new themes emerged. We reached thematic saturation for 46 participants. Our approach aligns with prior work [62]. Finally, we created 7 higher-level themes that explained the decision-making process of our participants—*security concerns, trust, need, digital literacy, serious and observant, outliers, and preferences*. The full theme hierarchy is in Appendix I).

6 Results

To set the context of the analysis, we first investigated if our participants were aware of the UPI frauds.

Awareness about UPI frauds: All except one participant reported that they are aware of UPI frauds and shared personal experiences. These participants shared stories of friends who were victims of UPI-fraud: (P7) *"A friend of mine once almost fell on such attack about a car scam."* Sometimes, there were specific topics that came up over and over again: (P14) *"I and many of my friends have been called by someone saying that I'm from SBI, these are your debit card details and something like that."* Participants also reported that they (P7) *"have heard of such cases from the media"*, another rich source of information.

Experiencing UPI frauds in social circles: Four participants mentioned close family members falling victim to UPI frauds. However, two of them also reported being able to assist their family members: (P14) *"Even my father was a victim. That patron scam was running. They call you and say you have won a car. If you complete such formalities, you will get money and a car. We just walked away."* Only two participants reported being targets of fraud themselves. P14 explained, *"I was asked that I will be receiving this money and rather than they did the same thing, they give me a request."* This was a common approach where UPI users thought they were receiving money, but in reality, it was a request to pay money. Similarly, P2 also encountered such a situation.

While falling victim could possibly be under-reported due to phenomena such as desirability bias [42], causing participants to avoid admitting to succumbing to fraud, it is clear that participants were made aware of UPI-fraud at least from their social circles. In fact, almost all participants, irrespective of their demographics, expressed that they had experienced or knew someone who had

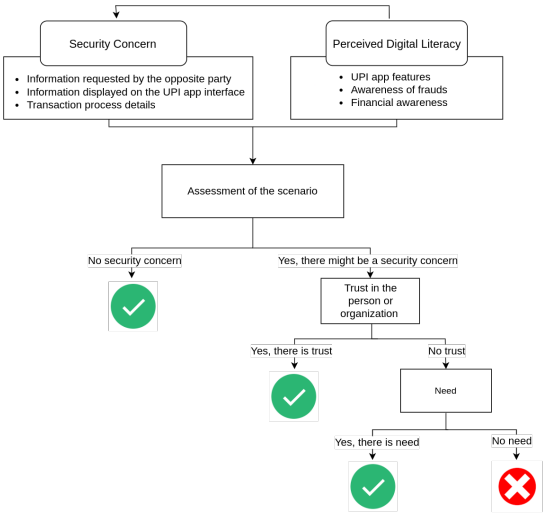


Figure 3: Multi-stage decision making process of UPI users while making a transaction.

experienced UPI fraud. Thus, we check how our participants make the decision of whether or not to go ahead with a UPI transaction.

6.1 RQ1: What is the Users' Decision-Making Process During a UPI Transaction?

We studied participants' decision-making process while using the UPI app in order to uncover their mental models. By analyzing their verbalized reasons for taking each action across multiple scenarios, we discovered that participants engaged in a common multi-stage decision-making process, illustrated in Figure 3. First, they assessed the situation to decide if there is a security risk based on an assessment of three aspects. However, if the participant felt a lack of digital literacy to identify security issues, even then, they were concerned.

If participants decided that there could be a security concern with the transaction, they then decided whether they trusted the individual/organization with whom they were engaging. Trust would lead them to ignore the security concern. However, even if they did not trust the other party, if there was a very pressing need they proceeded anyway. In this section we detail the full decision-making process.

6.1.1 Deciding if there could be a Security Risk. The first decision-making step that participants performed was to decide whether they felt concerned about the security of the transaction. They did this by considering three aspects of the situation.

Three criteria assessment of security risk: One, they considered the face validity of the larger scenario. This came in the form of deciding if it made sense to carry out this transaction using UPI. For instance, P18 was concerned about being solicited over a phone call and thus not having a record of the transaction purpose: *"But without receipt or without getting the item is what I mean, I will not go for payment."* P8 similarly was suspicious about someone reaching out over the phone because of their past experience: *"I won't be paying to a bank account over a call and instead go to the company's portal for paying the money. I would not believe in anyone who says that he is from customer care."*

Two, users considered the necessity of the information requested. For example, they evaluated whether it is necessary to share certain details about the bank account, which were personal, or disclose recent transactions. For example, P12 pointed out that on *"SMS: don't share OTP"* (One-Time Password), since this raises a security concern.

Three, they looked for a mismatch between the situation and the information reflected on the app interface. Checking the amount of money being paid was common: (P10) *"And this is the amount. After checking the amount, I can just validate that transaction by entering my UPI PIN."* Additionally, users checked that the recipient was correct, the bank account being used for payment was known, the link was indeed used for payment, and the details in the notification were accurate. All participants meticulously engaged in this step.

Impact of digital literacy on risk assessment: Many participants drew on their prior experience of UPI fraud and their digital literacy skills to be able to identify whether the above three aspects of the situation were problematic. Literacy in **fraud mechanisms** allowed users to detect issues. P1 explained that it's *"dangerous for me to click to any random link"* and exercised healthy suspicion of requests to do so. Literacy of **financial transactions** was also used to diagnose whether the transaction made sense. P4 reasoned in one scenario, *"There should be proof that we have invested. If later I need to refund something or I don't want to invest for more days, then I can show the proof that I had invested in this, and you should return it to me."* Making a payment without that proof seemed suspicious. Finally, literacy of **UPI app features** also had an impact. It influenced understanding the difference between the features for paying and receiving funds: (P1) *"I would never have to accept the request to get some money into my account."*

In fact, 45 out of 46 participants believed a lack of digital literacy could make them more susceptible to fraud. For example, P14 remarked *"More old people are vulnerable to such attacks. If people are using such apps, then they will be vulnerable because they are not aware of the ground rules at all"*. Moreover, P13 highlighted that *"I think tech savvy, people, I think they will not fall for stuff like this"*.

Previous work identified that users leverage digital literacy about security risks, use of situational cues, and perceptions of negative consequences while deciding whether to click on a phishing link [40]. Our work resonates with these findings. However, we also identify the significant impact of trust on receivers as well as the need to go ahead with the financial transaction (a potential positive consequence) on the decision-making process of UPI users, which has not been explored earlier. We will discuss them next.

6.1.2 Impact of Trust and Need. **Trust in a recipient results in proceeding with the transaction**: Participants who felt concerned about a scenario then considered whether they trusted the recipient. 45 out of 46 participants stated the importance of trusting the receiver. If the participant trusted the individual or organization, they would proceed with the UPI transaction. Without trust, participants would not want to proceed. P10 expressed, *"I am not comfortable with this transaction, so I will not continue. I find this phone call thingy a little shady so I won't go along this transaction"*.

While often this was the final decision point, there was a rare but powerful factor of need and urgency that drove some users to proceed with the transaction anyway.

Impact of need: Three participants felt such a pressing need to engage in the transaction that it outweighed their reluctance up to this point. Despite their security concern and a lack of trust in the other party, these users proceeded with the UPI transaction: (P13) *"So this one I am paying them. Right. So I think I can go ahead and pay them. So that's right. I'm trying to pay them because I want some item. So I'll just go ahead and pay them."* In such vulnerable situations, 5 out of 30 users had a tendency of giving the benefit of the doubt to the receiving entity to justify their decision, which may or may not have led to a safe transaction. (P9) *"Yeah. So assuming all that website being legit and all, I'll pay it from here."*

6.1.3 Post Scenario Reflection. After each participant had completed all of the scenarios, we shared with them whether they had fallen for fraud. We also educated them on the various types of fraud. Participants then reflected on their behavior while encountering these scenarios–some of them were new to some participants.

Some participants perceived a lack of digital literacy: While reflecting, several users were candid to share how their lack of digital literacy led to a mistaken decision during the study: (P5) *"I never thought there will be a fraud thing goes on with the URL thing."* Here, P5 fell for fraud since they lacked awareness of this way of committing fraud and so were not suspicious of the link. P3 was unfamiliar with certain UPI functionality: *"I don't know that we can link different accounts with the same number."* This lack of knowledge proved problematic during a fraudulent UPI transaction.

Compelling need might override assessed security risk: A few participants reflected that they indeed detected a security risk, but ended up ignoring their security concerns. They went ahead and proceeded with the UPI transaction when the need was compelling enough. In fact, 16 of the participants shared in their post-reflection that they were aware of people (in their social circles or the news) who had been deceived due to the urgency of the situation.

6.2 RQ2: What are the User Preferences to Enhance the Design of UPI Apps to Improve Protection Against Fraud?

In this section, we will discuss the preferences of UPI users towards nudges, the reasons for their choices, and the new features for UPI apps as suggested by users. In our study, we asked the users to rate a given set of nudges as per the effectiveness perceived by them. To that end, we will report results regarding the four nudge designs–two types of notifications *viz.* "view-once notification" (Fig. 2f) and "screen-blocking notification" (Fig. 2e), "badges" (red, yellow, green for flagged, unverified and verified respectively) (Fig. 2b, 2c, 2d) and "Amount will be deducted"(Fig. 2a). We also show results for the control condition–no nudges.

6.2.1 Badges is the Most Preferred Nudge by Our Participants. We present the mean and median of user-reported ratings for the nudges in Table 6. Notably, among all nudge designs, "Badges" emerged with the highest ratings consistently across all 46 participants — it obtained mean and median ratings of 8.26 and 8.5 respectively.

Nudge Design	Mean Rating	Median Rating
Badges	8.26	8.5
Screen-blocking notification	7.67	8
Amount will be deducted	7.08	8
View-once notification	7.14	7
No Nudge	4.78	5

Table 6: Different nudges with their mean and median preference ratings (out of 10) provided by our 46 participants.

The "Amount-will-be-deducted" nudge contains design flaws: Participants highlighted design flaws and improvements for "Amount-will-be-deducted" in our qualitative analysis. "Amount-will-be-deducted" was designed to address a lack of digital literacy and transaction awareness (Table 4)—user decisions and feedback indicate that although the information was useful, it was not well communicated. P22 mentioned that *"...rather than having amount will be deducted below the description, we can have either it at the above the cost or just at the top of the notification"*.

Reinstating trust in the recipient is the primary reason for preferring Badges: The "Badges" were the most preferred nudge for the majority of our participants because it reinstates trust of users in the receiver. As admitted by certain users (P2) *"Badges are there, they signal whether it's right or wrong."* This is in line with our earlier results in RQ1, which found that trust is a major intrinsic factor that affects the decision-making process of an individual. In the same vein, P12 mentioned *"If I know him and trust him I would pay"* and P3 expressed *"We won't pay someone we don't know"*.

Suggestions to Improve Badges: We further asked our participants if they had suggestions to improve "Badges". The suggestions varied across two dimensions–First, along with suggestions for better authentication. P10 mentioned that *"we can link this app with some features which will allow us to authenticate whether this person is a valid representative or not"* while P2 suggested *"First, there should be verification, then it should be a 'pay' or 'not.' Yes/No, then Pay/Decline"*. Secondly, participants also provided suggestions for improving the design of "Badges"—P7 mentioned *"The verified symbol should be big or come as a popup"* while P13 remarked *"those red flags I think should be a bit like more bigger"*.

Previous work (that we also used to find and categorize our nudges) identified that deploying nudges might be difficult as the users might confuse them with other interface elements [45]. Our findings are in line with them. However, building on this work, we further found the utility of specific nudges in our context, e.g., nudges like "Badges" which combine educational awareness (trustworthiness of receivers) represented by a color coded user interface elements are appreciated by our participants and deemed to be useful.

6.2.2 UPI Users Preferred Screen-Blocking as a Notification Nudge. Within notifications, "screen-blocking notifications" are preferred over "view-once notifications", with the mean and median ratings being 7.67 and 8 respectively. We investigated the reason for this user preference using qualitative data.

Nudging towards meticulous validation of information is easier with screen-blocking notification: The user responses

revealed that the screen-blocking notification nudged individuals towards a meticulous review of transaction details such as amount, account, receiver, and sender information. In particular, P5 highlighted *"Okay, if I am going to pay through QR, I will make sure whether the name is correct or not of the scanner, the name which I got of the scanning. If I am paying to a number I will recheck them"*. Thus, "screen-blocking" notifications facilitated heightened awareness, prompting users to verify critical information that they deemed essential for protecting against fraud. Another significant reason is that "screen-blocking" notifications encouraged users to check for money or process mismatches, which was desired by them. P1 mentioned *"Since I have to pay them INR 1500, why would they need my UPI ID? So I will ask for that UPI ID and not give them my mobile number"*. Conversely, users perceived that "view-once notifications" did not prompt them sufficiently to make the necessary checks, particularly compared to the "screen-blocking" notification.

7 Design Implications

So far, our analysis identified that nudges impact users' decision-making process. However, while reviewing and rating these nudges, users identified concrete improvements for them, as well as sought novel intervention and assistance mechanisms. We realized that these suggestions can provide an acute roadmap for stakeholders of the UPI ecosystem to improve the usability as well as security of UPI apps. Thus, we take a systematic qualitative approach to synthesize concrete design implications from our data. We grouped all the quotations that fall into the category of suggestions by users, insights given by users during the interview, and preferences of the users. Next, 2 researchers collaboratively read the quotations to identify that, besides minor modifications in nudge design to improve visibility and increase optimal friction during a transaction, UPI users desire 2 specific types of novel assistance to combat fraud.

7.1 Assistance for Raising User Awareness

Providing education/ customer guideline for combating frauds: Participants emphasized the critical role of education in fostering awareness and vigilance regarding various types of frauds and the use of UPI apps. They mentioned that such training will enable them to effectively identify and mitigate fraud. For example, P15 mentioned *"people should firstly know about what is happening around them, what sort of attacks can happen"*. In addition to it, some of them want support from the companies (e.g., Google) providing UPI services in the form of guidelines to the users to be safe and tutorials regarding the proper usage of the app— P10 mentioned that *"They should also have some help lines or certain guidelines like they can upload some tutorials on how to use it, what to be careful about and what to step might be confusing. These guidelines can be referred"*.

Providing customized nudges based on transaction amount and age of user: When users were asked for suggestions and insights to improve the UPI interface, they highlighted the importance of providing contextual nudges based on factors such as transaction amount and user demographics to balance usability and security. For instance, some users suggested implementing additional steps for larger transactions—(P10) *"One suggestion was like adding an additional step, for example, for larger amounts we can add more steps before we actually make the transaction"*. Moreover, users emphasized the need for parental/caregiver verification controls for minors and elderly individuals, with suggestions such as limiting transaction capabilities—(P11) *"For individuals who need some guardian control, we can have a feature that prevents them from resetting it for another week or so"*. P14 mentioned *"More elderly people are vulnerable to such attacks. If they are using such apps, they will be vulnerable because they are not aware of the ground rules at all"*. We did not observe any such preferences based on other factors such as gender and experience with UPI apps.

7.2 Assistance to Attain More Trust in the Recipients

The existing functionality to see user-specific transaction history can only help with known recipients. However, scammers might often exploit unknown UPI accounts. To that end, our participants expressed the need to establish the authenticity of the person with whom they are making a transaction. Their suggestions ranged from having a profile image and profile display feature, having verification "Badges" (in coherence with our study design), and being vigilant at the time of transaction. However, their call to establish the trustworthiness of UPI accounts is a non-trivial problem. If a UPI app uses crowdsourcing to assess such trustworthiness, then malicious actors might exploit the system to mark even good UPI accounts as untrustworthy. However, we also realized that this need provides a unique research opportunity to create tools and techniques assigning trust scores to UPI accounts. Our insight is that UPI, unlike social networking platforms, has a well-regulated higher barrier of entry—each account must have a bank account and phone number. To that end, banks routinely identify malicious accounts based on their transaction pattern [33]. Based on this ground truth of malicious accounts, UPI developers can conduct extensive research to detect malicious accounts on online platforms. Specifically, they can leverage *Sybil resistant online content voting*, *Sybil tolerant* schemes, and even account registration information (before accounts perform any transaction) to assign trust score to UPI accounts [78, 81, 85].

8 Discussion

In this work, we identify the ever-growing concern of fraud for Indian users on UPI apps. To combat these frauds, UPI apps developed and deployed interface nudges to alert users and protect them from frauds, but we identified the lack of a systematic study discussing the impact of these interface nudges to manage frauds. To that end, in this work, we designed and built a UPI app simulator called UPI-Pay and used this system to conduct the first study to identify the susceptibility of users towards fraudulent transactions on UPI and the effectiveness of nudges against these frauds. We discuss and contextualize the implications of our key results below.

Novel understanding of decision making process in UPI transactions: We are the first study to uncover a systematic decision-making process of users (to answer RQ1) based on tension between user literacy, security concern, user need and trust of the recipient. Our findings reveal that UPI users might continue with a transaction if they feel there is a need for the transaction (e.g., obtaining

some gift). So, these users are motivated by possible positive consequences as well as trust in the receiver. This is different from earlier work [40] on phishing attacks. A possible reason for our novel observation might be our unique context. In UPI transactions, users expect instant gratification, rather than delayed consequence (e.g., for clicking on a phishing link) since there is money involved. This sense of immediate monetary gratification might significantly impact the decision-making process compared to other scams (e.g., phishing). The importance of trust as a mental model is aligned with a prior study that highlighted the lack of trust in the UPI platform and people as a key concern of UPI users. Our study additionally captures the behavior of users during a series of simulated transactions and establishes the sequence of considerations in the process of making a transaction using UPI (Section 6.1).

Measuring relative effectiveness of different security nudges to combat UPI fraud: Based on the extensive research on nudges, it might have been imaginable that the nudges deployed in UPI interfaces have *some* impact on user decision and behavior. Our study showed that users were significantly less likely to fall for fraud when there were nudges present in the interface, making correct decisions 82.58% of the time (i.e., allowing non-fraudulent transactions while blocking fraudulent transactions) as compared to 65.38% of the time for scenarios with no nudge. However, the user feedback session rated the nudges quite unevenly (via ratings and qualitative responses), making "Badges" the most preferred nudge. Participants also suggested minor modifications in the design of some nudges and novel intervention mechanisms. Note that our work gives rise to an interesting question—when all of these nudges are deployed in the real world, are they helping the UPI users already? Our results indicate that they possibly do, however, there is tremendous scope for improvement. To that end, there is scope for future work to compare the efficacy of different interface nudges in the UPI apps and analyse if the enhancements suggested by participants of our study improve their safety against fraud attempts via UPI apps. We encourage developers to come forward to systematically design, build, and deploy improved nudges to help users make instant payments safely.

Assisting users to quantify the trust they should put on other UPI accounts: While checking the user ratings on different nudges, we identified an alignment with trust. Participants identified "Badges" to build trust in the receiver and rated it the highest (8.26/10) nudge during the experiment. This finding is in line with prior work, which states that individuals seek trust in the parties involved in the transaction [60]. However, establishing this trust to address the user need in a nontrivial problem–it requires a combined effort from stakeholders of the UPI ecosystem, the government, banks, developers, and security researchers to recognize and address this issue. We already identified a few key avenues through which such trust-establishing systems can be built (Section 7).

9 Future Work

Our work highlighted the decision-making process and usability preferences of UPI app users in India. It also captured users' interaction with nudges and a variety of scenarios that underscored the importance of trust and need backed by their digital literacy. We encourage researchers to conduct quantitative studies on the comparative efficacy of nudges as deployed in real-world apps. This will further assist developers to improve the interface designs and build more secure and usable payment apps. Further an at scale usability study deployed across India could help understand the cultural influence on decision-making of users on peer-to-peer instant payment apps. The same can be extended globally to countries that have begun to use UPI-based apps and study the difference in behavior and preferences towards instant financial transactions. A deep understanding of user mental models followed by a trend analysis of development in user behaviour with time, has the potential to facilitate policy modifications for instant payment systems. We strongly believe that this work will assist novel future research to solve the inconvenience and distress of end users and help hundreds of millions to make quick and safe peer-to-peer payments by designing and building secure and usable payment infrastructures.

10 Acknowledgments

We extend our sincere appreciation to Manaswi Raj, Rajdeep Ghosh, and Hardik Pravin Soni for their valuable help in conducting interviews. We also thank the anonymous reviewers for their feedback. This work is partially supported by a Google Academic Research Award (GARA) and a Google India faculty research award.

References

[1] About Google Pay. https://pay.google.com/about/. [Online; accessed 15 Dec. 2025].
[2] BBB® Online Purchase Scams Report, 2021. https://www.bbb.org/content/dam/bbb-institute-(bbbi)/2021-online-purchase-scams/Final%202021-BBB-OnlinePurchaseScamsReport.pdf. [Online; accessed 15 Dec. 2025].
[3] Financial fraud top cyber crime in India; UPI, e-banking most targeted: Study - Hindustan Times. https://www.hindustantimes.com/business/financial-fraud-top-cyber-crime-in-india-upi-e-banking-most-targeted-study-101695036325725.html. [Online; accessed 15 Dec. 2025].
[4] FINDINGS FROM A PILOT STUDY TO MEASURE FINANCIAL FRAUD IN THE UNITED STATES. https://longevity.stanford.edu/wp-content/uploads/2017/02/SCL-Fraud-Report-Feb-2017_Draft2.pdf. [Online; accessed 15 Dec. 2025].
[5] How do i transfer funds to my bank account? https://www.paypal.com/in/cshelp/article/how-do-i-transfer-funds-to-my-bank-account-help394. [Online; accessed 15 Dec. 2025].
[6] . Making Money vs. Managing Money: India's Critical Financial Literacy Gap . https://www.business-standard.com/content/specials/making-money-vs-managing-money-india-s-critical-financial-literacy-gap-125021900786_1.html. [Online; accessed 15 Dec. 2025].
[7] Olx is full of UPI scammers. https://www.reddit.com/r/india/comments/115r6l5/olx_is_full_of_upi_scammers/. [Online; accessed 15 Dec. 2025].
[8] Payments Fraud and Control Report. https://www.jpmorgan.com/content/dam/jpm/commercial-banking/insights/cybersecurity/highlights-afp-2022-payments-fraud-and-control-report.pdf. [Online; accessed 15 Dec. 2025].
[9] Paypal. https://www.paypal.com/in/home.
[10] Paytm. https://paytm.com/. [Online; accessed 15 Dec. 2025].
[11] PhonePe. https://www.phonepe.com/. [Online; accessed 15 Dec. 2025].
[12] Survived UPI scam that happened on OLX . https://www.reddit.com/r/IndianGaming/comments/wwkw6c/ama_survived_upi_scam_that_happened_on_olx/. [Online; accessed 15 Dec. 2025].
[13] UPI Ecosystem Statistics - National Payments Corporation of India (NPCI). https://www.npci.org.in/what-we-do/upi/upi-ecosystem-statistics. [Online; accessed 15 Dec. 2025].
[14] UPI Product Statistics - National Payments Corporation of India (NPCI). https://www.npci.org.in/what-we-do/upi/product-statistics. [Online; accessed 15 Dec. 2025].
[15] Venmo Payment App. https://venmo.com/about/us/. [Online; accessed 15 Dec. 2025].
[16] Venmo: Standard Bank Transfers FAQ. https://help.venmo.com/hc/en-us/articles/235399967-Standard-Bank-Transfers-FAQ. [Online; accessed 15 Dec. 2025].
[17] Victim of upi fraud. https://www.reddit.com/r/india/comments/wcj7gs/victim_of_upi_fraud_need_advice/. [Online; accessed 15 Dec. 2025].

[18] Zelle. https://www.zellepay.com/. [Online; accessed 15 Dec. 2025].

[19] 75% of Consumers Who Use Online Bank Transfers Worry About Fraud - PYMNTS.com. https://www.pymnts.com/news/payment-methods/2023/75percent-of-consumers-who-used-online-bank-transfers-are-concerned-about-fraud-risk, April 2023. [Online; accessed 15 Dec. 2025].

[20] Economic Survey 2023: UPI accounted for 52% of India's total digital transactions in FY22. https://www.moneycontrol.com/news/business/economic-survey-2023-upi-accounted-for-52-of-indias-total-digital-transactions-in-fy22-9970741.html, Jan 2023. [Online; accessed 15 Dec. 2025].

[21] Faster Payments, Faster Fraud: Examining the Challenges of Faster Payment Systems' Mass Adoption in India, the UK, Malaysia, and Australia - Outseer. https://www.outseer.com/fraud-protection/faster-payments-faster-fraud-examining-the-challenges-of-faster-payment-systems-mass-adoption-in-india-the-uk-malaysia-and-australia, September 2023. [Online; accessed 15 Dec. 2025.

[22] Mitnick, K., & Simon, W. (2002). The art of deception Controlling the human element of security. New York, New York Wiley Publishing. - References - Scientific Research Publishing, 2023. [Online; accessed 15 Dec. 2025].

[23] Xcode | Apple Developer Documentation, July 2023. [Online; accessed 25 Dec. 2025].

[24] Mobile Operating System Market Share India . https://gs.statcounter.com/os-market-share/mobile/india, January 2024. [Online; accessed 15 Dec. 2025].

[25] India: UPI usage by platform Statista. https://www.statista.com/statistics/1034443/india-upi-usage-by-platform, 2025. [Online; accessed 15 Dec. 2025].

[26] India's upi fraud count. https://razorpay.com/blog/upi-frauds-types-tactics/., February 2025. [Online; accessed 15 Dec. 2025].

[27] India's upi revolution. https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=154912&ModuleId=3, July 2025. [Online; accessed 15 Dec. 2025].

[28] Aadhaar: Unique Identification Authority of India. https://uidai.gov.in/. [Online; accessed 15 Dec. 2025].

[29] Abigail Bosze. How many people use Venmo in 2024? https://www.doofinder.com/en/statistics/how-many-people-use-venmo. [Online; accessed 15 Dec. 2025].

[30] Alessandro Acquisti, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Manya Sleeper, Yang Wang, and Shomir Wilson. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Comput. Surv.*, 50(3), August 2017.

[31] Maghsoud Amiri and Siavash Hekmat. Banking fraud: a customer-side overview of categories and frameworks of detection and prevention. *Journal of Applied Intelligent Systems and Information Sciences*, 2(2):58–67, 2021.

[32] Mohit Bansal, Shekhar Lele, Ashish Punjabi, and Pooja Lad. UPI 2.0: Towards a complete digital ecosystem. https://www.pwc.in/industries/financial-services/fintech/fintech-insights/upi-2-0-towards-a-complete-digital-ecosystem.html.

[33] Daniela-Georgeta Beju and Codruța-Maria Făt. Frauds in banking system: Frauds with cards and their associated services. In *Economic and Financial Crime, Sustainability and Good Governance*, pages 31–52. Springer, 2023.

[34] Divya Bhati. Statistics of UPI frauds in India in 2023. https://www.indiatoday.in/technology/news/story/more-than-95000-upi-fraud-cases-reported-in-2022-here-is-how-you-can-stay-safe-2386084-2023-05-29, May 2023. [Online; accessed 15 Dec. 2025].

[35] Marilyn Hughes Blackmon, Peter G. Polson, Muneo Kitajima, and Clayton Lewis. Cognitive walkthrough for the web. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'02)*, page 463–470, 2002.

[36] Walid Briki and Olivier Hue. How red, blue and green are affectively judged. *Applied Cognitive Psychology*, 30, 11 2015.

[37] Business Today. Year ender 2023: UPI transactions rose 147% in 5 years; new features announced in 2023: NPCI, RBI. https://www.businesstoday.in/personal-finance/news/story/year-ender-2023-upi-transactions-rose-147-in-5-years-new-features-announced-2023-npci-rbi-411350-2023-12-30, 2023. [Online; accessed 15 Dec. 2025].

[38] Cristina Liviana Caldiroli, Francesca Gasparini, Silvia Corchs, Andrea Mangiatordi, Roberta Garbo, Alessandro Antonietti, and Fabrizia Mantovani. Comparing online cognitive load on mobile versus PC-based devices. *Pers. Ubiquit. Comput.*, 27(2):495–505, April 2023.

[39] Lokesh Choudhary. Statistics of UPI. https://analyticsindiamag.com/believe-it-or-not-55-of-digital-frauds-happen-via-upi/, May 2023. [Online; accessed 15 Dec. 2025].

[40] Julie S Downs, Mandy Holbrook, and Lorrie Faith Cranor. Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, pages 37–44, 2007.

[41] Education and Careers Desk. IIT Madras working on voice-based contact-less payment services which recognises local Indian languages. https://www.news18.com/news/education-career/iit-madras-working-on-voice-based-contact-less-payment-services-which-recognise-i-3744068.html, May 2021. [Online; accessed 15 Dec. 2025].

[42] Robert J Fisher. Social desirability bias and the validity of indirect questioning. *Journal of consumer research*, 20(2):303–315, 1993.

[43] Flipkart. Scam Advisory: Beware of fraudulent sites and fake offers misusing Flipkart's name. https://stories.flipkart.com/fake-offers-fraudulent-sites-2/. [Online; accessed 15 Dec. 2025].

[44] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. Do or do not, there is no try: user engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 97–111, 2016.

[45] Franz, Anjuli and Zimmermann, Verena and Albrecht, Gregor and Hartwig, Katrin and Reuter, Christian and Benlian, Alexander and Vogt, Joachim. SoK: Still Plenty of Phish in the Sea—A Taxonomy of User-Oriented Phishing Interventions and Avenues for Future Research. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 339–358, 2021.

[46] Divya Guha. UPI surges; now 51% of digital transactions in India. https://www.fortuneindia.com/macro/upi-surges-now-51-of-digital-transactions-in-india/106290, Dec 2021. [Online; accessed 15 Dec. 2025].

[47] Yasmeen Hanif and Harjinder Lallie. Security factors on the intention to use mobile banking applications in the UK older generation (55+). A mixed-method study using modified UTAUT and MTAM - with perceived cyber security, risk, and trust. *Technology in Society*, 67:101693, 11 2021.

[48] Gunnar Harboe and Elaine M. Huang. Real-World Affinity Diagramming Practices: Bridging the Paper-Digital Gap. In *Proceedings of the 2015 CHI Conference on Human Factors in Computing Systems*, CHI '15, 2015.

[49] Sumair Ijaz Hashmi, Rimsha Sarfaraz, Lea Gröber, Mobin Javed, and Katharina Krombholz. Understanding the security advice mechanisms of low socioeconomic pakistanis. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, CHI '25. Association for Computing Machinery, 2025.

[50] Jason Hong. The state of phishing attacks. *Communications of the ACM*, 55(1):74–81, 2012.

[51] Markus Jakobsson, Alex Tsow, Ankur Shah, Eli Blevis, and Youn-Kyung Lim. What instills trust? a qualitative study of phishing. In *Financial Cryptography and Data Security*, pages 356–361, 2007.

[52] Debora Jeske, Pam Briggs, and Lynne Coventry. Exploring the relationship between impulsivity and decision-making on mobile devices. *Pers. Ubiquit. Comput.*, 20(4):545–557, August 2016.

[53] Katie Marriner. India is overtaking China today as the world's most populous country – according to this projection. https://www.marketwatch.com/story/india-is-overtaking-china-today-as-the-worlds-most-populous-country-according-to-this-projection-d268ead9. [Online; accessed 15 Dec. 2025].

[54] Aarzu Khan. NPCI's voice-based payment solution could be a game changer. https://dazeinfo.com/2021/07/21/npcis-voice-based-payment-solution-could-be-a-game-changer/, Jul 2021. [Online; accessed 15 Dec. 2025].

[55] Renuka Kumar, Sreesh Kishore, Hao Lu, and Atul Prakash. Security analysis of unified payments interface and payment apps in India. In *Proceedings of the Usenix Security Symposium 2020*, 2020.

[56] Athul Kuriakose, PB Sajoy, and Elsa George. Modelling the consumer adoption intention towards unified payment interface (upi): An extended utaut2 model with relative advantage, add-on services and promotional benefits. In *2022 Interdisciplinary Research in Technology and Management (IRTM)*, pages 1–7. IEEE, 2022.

[57] Sevinc Kurt and Kelechi Kingsley Osueke. The effects of color on the moods of college students. *SAGE Open*, 4(1):2158244014525423, 2014.

[58] Daniele Lain, Tarek Jost, Sinisa Matetic, Kari Kostiainen, and Srdjan Capkun. Content, nudges and incentives: A study on the effectiveness and perception of embedded phishing training. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, CCS '24, page 4182–4196, 2024.

[59] Thomas C Leonard. Richard H. Thaler, Cass R. Sunstein, Nudge: Improving decisions about health, wealth, and happiness: Yale University Press, New Haven, CT, 2008, 293 pp, $26.00, 2008.

[60] Feng Li, Dariusz Pieńkowski, Aad van Moorsel, and Chris Smith. A holistic framework for trust in online transactions. *International Journal of Management Reviews*, 14(1):85–103, 2012.

[61] Maestra. https://maestrasuite.com/. [Online; accessed 15 Dec. 2025].

[62] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. Reliability and inter-rater reliability in qualitative research: Norms and guidelines for cscw and hci practice. *Proceedings of the ACM on human-computer interaction*, 3(CSCW):1–23, 2019.

[63] Mary L McHugh. Interrater reliability: the kappa statistic. *Biochem Med (Zagreb)*, 22:276–82, 03 2012.

[64] Shweta Mudaliar. Over 95,000 UPI fraud cases reported in 2022-23: Centre in Parliament. https://www.hindustantimes.com/india-news/over-95-000-upi-fraud-cases-reported-in-2022-23-centre-in-parliament-101679541121388.html, Mar 2023. [Online; accessed 15 Dec. 2025].

[65] Deepthi Mungara, Harshini Sri Ramulu, and Yasemin Acar. Security and Privacy Advice for UPI Users in India. In *Proceedings of the Usenix Security Symposium 2025*, pages 6085–6103, 2025.

[66] James Nicholson, Lynne Coventry, and Pam Briggs. Can we fight social engineering attacks by social means? Assessing social salience as a means to improve

phish detection. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 285–298, 2017.
[67] NPCI. UPI: Unified Payments Interface - Instant Mobile Payments | NPCI. https://www.npci.org.in/what-we-do/upi/product-overview, February 2024. [Online; accessed 15 Dec. 2025].
[68] Norbert Nthala and Rick Wash. How Non-Experts Try to Detect Phishing Scam Emails. In *Workshop on Consumer Protection*, 2021.
[69] Times of India. Upi use among women low, assisted onboarding can drive uptake: Gpay's arati deo. https://economictimes.indiatimes.com/industry/banking/finance/upi-use-among-women-low-assisted-onboarding-can-drive-uptake-gpays-arati-deo/articleshow/100497224.cms?from=mdr, May 2023. [Online; accessed 15 Dec. 2025].
[70] PricewaterhouseCoopers. Combating fraud in the era of digital payments, February 2024. [Online; accessed 15 Dec. 2025].
[71] PYMNTS. PayPal Sees Jump in Transactions Per Account as Fastlane Checkout Boosts Conversions. https://www.pymnts.com/earnings/2024/paypal-branded-checkout-total-payment-volumes-jump-7percent-debit-drives-incremental-transactions/. [Online; accessed 15 Dec. 2025].
[72] Reserve Bank of India. https://www.rbi.org.in/. [Online; accessed 15 Dec. 2025].
[73] Aditi Routh. The Role of Nonbanks and Fintechs in Boosting India's UPI Person-to-Merchant Transactions. https://www.kansascityfed.org/research/payments-system-research-briefings/the-role-of-nonbanks-and-fintechs-in-boosting-indias-upi-person-to-merchant-transactions/, August 2024. [Online; accessed 15 Dec. 2025].
[74] Salary Explorer. Average Salary in India 2023. https://web.archive.org/web/20230705111605/https://www.salaryexplorer.com/salary-survey.php?loc=100&loctype=1. [Online; accessed 15 Dec. 2025].
[75] santander trade markets. India: Economic and political outline. https://santandertrade.com/en/portal/analyse-markets/india/economic-political-outline. [Online; accessed 15 Dec. 2025].
[76] The Hindu. With 220mn users, India is now world's second-biggest smartphone market. https://www.thehindu.com/news/cities/mumbai/business/with-220mn-users-india-is-now-worlds-secondbiggest-smartphone-market/article8186543.ece.
[77] The Times of India. The Rise of UPI: Transforming the way Indians transact. https://timesofindia.indiatimes.com/blogs/voices/the-rise-of-upi-transforming-the-way-indians-transact/, July 2023. [Online; accessed 15 Dec. 2025].
[78] Dinh Nguyen Tran, Bonan Min, Jinyang Li, and Lakshminarayanan Subramanian. Sybil-resilient online content voting. In *NSDI*, volume 9, pages 15–28, 2009.
[79] Clive Unger, Dhiraj Murthy, Amelia Acker, Ishank Arora, and Andy Chang. Examining the evolution of mobile social payments in venmo. In *International Conference on Social Media and Society*, pages 101–110, 2020.
[80] Maximilian Valta and Christian Maier. Digital nudging: A systematic literature review, taxonomy, and future research directions. *SIGMIS Database*, 56(1):101–125, January 2025.
[81] Bimal Viswanath, Mainack Mondal, Krishna P Gummadi, Alan Mislove, and Ansley Post. Canal: Scaling social network-based sybil tolerance schemes. In *Proceedings of the 7th ACM european conference on Computer Systems*, pages 309–322, 2012.
[82] Rick Wash. How experts detect phishing scam emails. *Proc. ACM Hum.-Comput. Interact.*, 4(CSCW2), October 2020.
[83] Wion. UPI goes global: The past, present & future of India's payments platform. https://www.wionews.com/business-economy/upi-goes-global-the-past-present-future-of-indias-payments-platform-630396. [Online; accessed 15 Dec. 2025].
[84] Michael Workman. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *JASIST*, 59:662–674, 02 2008.
[85] Dong Yuan, Yuanli Miao, Neil Zhenqiang Gong, Zheng Yang, Qi Li, Dawn Song, Qian Wang, and Xiao Liang. Detecting fake accounts in online social networks at the time of registrations. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, pages 1423–1438, 2019.
[86] zelle. Zelle soars with $806 billion transaction volume, up 28% from prior year. https://www.zellepay.com/press-releases/zelle-soars-806-billion-transaction-volume-28-prior-year. [Online; accessed 15 Dec. 2025].
[87] Xinyi Zhang, Shiliang Tang, Yun Zhao, Gang Wang, Haitao Zheng, and Ben Zhao. Cold hard e-cash: Friends and vendors in the venmo digital payments system. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 11, pages 387–396, 2017.
[88] Sarah Y. Zheng and Ingolf Becker. Checking, nudging or scoring? evaluating e-mail user security tools76. In *Proceedings of the Nineteenth USENIX Conference on Usable Privacy and Security*, SOUPS '23, 2023.
[89] Zoom Remote Control. https://support.zoom.us/hc/en-us/articles/201362673-Requesting-or-giving-remote-control. [Online; accessed 15 Dec. 2025].

A Instructions for study to identify UPI App functionalities

We present below the detailed survey of Paytm, GooglePay, PhonePe for Payment via Mobile number and Via QR code. The survey was performed by two researchers independently and then their observations were combined. We focus on making payments via the interface, since user decisions during this phase might result in sending money to attackers.

A.1 Instructions to download the UPI app of choice

1. Open Playstore (for Android phones) and Appstore (for iOS).
2. Search app name (i.e. Google Pay) and click on Install/ Get to download.
3. Register on app with phone number linked to your bank account. This will be completed after a verification OTP.
4. Create a numeric pin to make payments in the future (same as having an ATM Pin). Ready for use.

A.2 Instructions for payment via mobile number

1. Open the app by clicking on the icon on the phone screen
2. Find and click the icon to initiate payment to a new mobile number or existing contact.
3. Search for a trusted contact's name (use a pre-decided contact in the phone in the research group who will return the received money).
4. Out of the search result, find the correct one, confirm.
5. Note down what details show up on the following screen (e.g., a verified blue tick signifying a verified user on the app).
6. Find and click on the payment button, note down the details on the screen.
7. Try to proceed without entering an amount. Note interface element and error message.
8. Proceed with entering an amount of 1 inr for payment. note down the details on the screen.
9. If prompted for UPI pin, enter a wrong pin, and note the details shown on screen.
10. Enter the correct pin, and note the details shown on screen.
11. Note down the details in the screen shown (e.g., alert message, completion notice) till the payment is complete.

A.3 Instructions for payment via scanning a QR code

Each UPI app can create unique QR codes for an account for receiving payment. In the QR code the amount might or might not be specified. We repeat the steps below for two QR-codes, one with a preselected amount of 1 inr and one without.

1. Open the app by clicking on the icon on the phone screen
2. Find and click the button for scan & pay.
3. Note down the details of the screen shown.
4. Scan the QR code from a trusted research group member.
5. Note down the details on the screen, find and click the button to proceed to the next step.
6. Repeat the steps 9 to 11 of "Pay via mobile number" above

A.4 Instructions for payment via uploading a QR code

Each UPI app can also load images of QR codes from a phone gallery instead of scanning via camera (useful if the image is shared via another channel, e.g., messaging platform). Once loaded the UPI-app will read the QR code and function as if the QR code is scanned via camera. We checked these functionality by loading two images of QR codes—one with pre-selected payment of 1 int and one without.

1. Open the app by clicking on the icon on the phone screen
2. Find and click the button for scan & pay.
3. Note down the details of the screen shown.
4. Find and click on the button for uploading QR code or scanning it from photo Gallery
5. Note down the details on the screen, find and click the button to proceed to the next step.
6. Repeat the steps 9 to 11 of "Pay via mobile number" above

We closed the app after all of these payments above and analyzed the notes of the researchers.

B Working of UPI-Pay simulator

We demonstrate the working of UPI-Pay simulator app where participants perform a common action—"Pay via contact no." in Figure 1a, Figure 1b, Figure 1c, Figure 1d (similar mechanisms are implemented for all basic UPI functionalities in Table 9). The user first **Search Receiver** by entering the receivers' contact no. Then the user **enter transaction amount** and choose a bank account followed by **entering UPI PIN**, which is set to '0000' in the experiment and conveyed to the user. Finally UPI-App alerts the user with **completion status**—whether the transaction was successful, along with a transaction summary.

C Pre-interview Survey

We asked the following questions to the participants in the survey:

1. What is your age?
2. What is your sex?
3. Preferred language for the interview
4. Can you participate in the interview using a laptop/desktop with an internet connection?
5. For how long have you used UPI apps?
6. Which UPI App have you used most?
7. How frequently do you use any UPI app?
8. Please briefly explain (1 – 3 sentences) your primary purposes of using this app (e.g., buying groceries, using Uber) etc.
9. What is your approximate average transaction amount per transaction via UPI?
10. What is your approximate maximum transaction amount you have ever done via UPI?
11. Are you willing to participate in our interview on the effects of interface-design of the UPI apps in India? This interview will be conducted on zoom and will take approximately 1 hour. You will be compensated with an amazon gift card at the end of this study. If you are willing, please also let us know an email id to contact you for scheduling the interview.

D Script of the Semi-structured Interview

Confirm from users that they read and understood the risks and benefits mentioned in the recruitment form that they filled up and provided their informed consent. Ask to re-read if necessary.

This is an interview research study on the effect of interface design on user choices in UPI apps (e.g., Google pay, PhonePe, Paytm, BHIM). Our goal is to improve the usability of such apps. You will be compensated with an Amazon.in gift card (worth inr 300) at the end of the interview (interview to be conducted on zoom and will take approximately 60 minutes).

For the purpose of research we want to record your responses and UPI-Pay app interactions during the interview. Please say 'I consent to recording' if you are okay with it else say 'No, I do not consent to recording'.

Do you have any questions or doubts regarding the study?

For the first part of the study, we are testing the usability of mobile payment apps from your viewpoint. To test this we are not using your phone but a virtual phone in our own computer and would like you to try using it. We'll like to mention there is no real currency or transactions involved, and this app software exists only on our virtual phone. We will do an audio recording of this meeting but no video. (We give each person a different design permutation of the app)

D.1 Introduction to the UPI simulator

This is the device, You can move around with a cursor. Pressing the left button of your mouse will result in touching or tapping the phone screen, Hence you need to press it once for a tap and keep pressing and moving for swipes. The home button here will get you to your home screen and help you switch apps. Pulling down from up while pressing left click from here will open the notification centre. This app right here named "UPI Pay" is the UPI Application installed on this device. This is your UPI Pin. We'd like you to take 2-3 minutes and get acquainted with functions of this simulator and the UPI-Pay application. Please ask any doubts you have regarding the simulator or the app? And please speak aloud while thinking (Wait for 2-3 minutes)

Familiarizing the user to the simulator interface: Can you please do the following tasks (ask the following and if they aren't clear just explain it to them)

1. Go to home screen
2. Open the UPI Pay(UPI App)
3. Switch from this app to home screen
4. Open the Browser Application(Safari)
5. Open the notification centre

Testing their familiarity: Now we will ask you a few questions and ask you to use the interface in different situations. For the purpose of this study, please think aloud, that is speak everything you're thinking while using the interface. Please do the following tasks (mention one by one, If they don't know after trying, do tell them.):

1. In this simulator, make a transaction worth 100 inr to the following number 222 (mobile no.) which belongs to Rohan (Owner of that number).
2. There is a QR code stored in your photos app. In the simulator, you can do a transaction using such QR codes. Please make a transaction worth 100 inr to the QR stored in Photos app (Let them open the app and point to the correct qr). Yes, this one.
3. Where do you think the money is deducted/added to when a transaction is done?
4. How do you check your balance in this app?

D.2 Transaction Simulation

Now that you are a bit familiar with the simulator interface, we will move to the second part of this study. I will present you with some practical usage scenarios like you are transacting with someone. Given these scenarios please use the simulator just as you will do in real life when you are facing similar scenarios. Remember that please think aloud while you are using the app to let us know why you are doing it that way. Please also mention if you are making any assumptions about the scenario during interacting with the app. (Randomly choose five scenarios from the ten scenarios below):

1. **OLX QR mockup story (have both fraudulent and non-fraudulent versions):** You have been trying to sell an old bicycle on OLX, an online marketplace for second hand goods. You have been contacted by Charul, who lives in an army place and hence can't come to collect the item. Thus Charul promises to pay in advance if you send it as a delivery to him. You are comfortable with the price he is paying. Charul sent you a screenshot showing that they did pay your amount. However, you haven't received it. Charul, the buyer then tells you that there is some technical issue and then sends you a QR code worth 3,000 inr He guides you through the process to upload it on your payment app. How will you handle this situation?
2. **Attacker asks UPI phone number and sends a collect request deceiving it as receiving money:** You have been trying to sell an old bicycle on OLX, an online marketplace for second-hand goods. You have been contacted by Geet, who lives in a remote place and hence can't come to collect the item. They however promise to pay in advance if you send it as a delivery to him. You are comfortable with the price he is paying. They sent you a screenshot saying that they did pay your amount. However, you haven't received it. The buyer claims that there is some technical issue and asks for your UPI phone number. How will you handle this situation?
3. **Attacker pretending to be representative of Flipkart:** You received a call from a person who says they are a flipkart associate. Since you have been a regular user of flipkart you have received a cashback offer where you'll receive a 50% cashback on any purchase worth up to inr 5,000 the person asks you to add items to your cart and confirms them with you. They ask you for the screenshot of the final cart gateway to verify you. How will you handle this situation?
4. **Fraudster pretending to buy gold on your behalf:** You received a call from a person who says he is a UPI-Pay customer care. Z-Pay has launched a digital locker system where you can buy and store gold online and sell at any point of time at market cost. Due to a tax exemption buying gold via this way gives you a very lucrative price and you decide to invest 5000 inr. You receive this notification from the payment app. This is just an example. It can be other payments apps you use like google pay/paytm. How will you handle this situation?
5. **No Fraudster story:** You are trying to buy a table on Facebook marketplace, an online marketplace for goods. You contact Jasbeer, They live far away so you wish for the item to be delivered to you. You've agreed to pay 1500 inr in advance if they give you a receipt. They ask for your UPI phone number. How will you handle this situation?
6. **Vendor:** You go to a vendor (Bhagya General Store) and have brought items worth 1500 INR. You wish to pay him that money so he generates a QR code and shares it with you. For convenience, this QR code is in your gallery. How will you handle this situation?
7. **Online social media seller phishing(have both fraudulent and non-fraudulent versions):** You wish to buy a dress worth 1500 inr from a seller Daya Textiles Ltd. you found on Facebook marketplace. He sends you a link so that you can easily pay the amount. The link is in the messages app on this device. How will you handle this situation?
8. **E-commerce pay on delivery:** You have bought something from Amazon, a trusted e-commerce website worth 500 Rs via pay-on delivery method. You wish to pay this sum by UPI so the delivery person generates a QR code and shows it to you. For convenience, this QR code is in your gallery. How will you handle this situation?

D.3 Debriefing, Mitigation and Feedback

Tell (Debrief) each person about the attack's attempts previously and whether they mitigated it correctly or not. Now we ask them the following (for each attempted attack): How do you think you should have mitigated it or ideally handled this case? Why do you think this will be better?

If they mention different reactions of different demographics, we will let them as it'll be of use later. (If the flipkart story is attempted) Flipkart never attempts any such thing. Flipkart or any other famous brand logo is just sometimes used by scammers to gain your trust. Hence it was used to see how trust created by the logo affects your decisions.

1. What do you think can help you to avoid falling to such attacks? If they don't mention it, ask from an application design perspective.
2. Have you or anyone you know ever been a victim of such attacks? How did they mitigate them? Please mention those incidents.
3. What and why did you or the other person face this attack? (Do get to know the source of how they know about these: news or tv/movie of public interest SMS/messages or personal experience)
4. Do you think any of your past experiences affected how you reacted to these stories or any UPI decision? Please take your time to recall (give them time to think and recall)
5. Do you tend to use different bank accounts and use some of them for UPI? If so, why?
6. Explain that some people do it as a security measure. Do you also have a checklist or some steps you have taken to be safe while doing UPI/banking-related transactions?
7. We will show you some variations in the design of this app, please rate each on how helpful you think it can be to avoid attacks on a scale of 1-10: a) verified/reported symbol - no symbol and symbol b)UPI Pin page c)View-once notification d)Screen-blocking e)Nothing

Thanks for your time and insights. As a token of gratitude we'll send the Amazon gift card. Do you want to receive it in this mail itself or a different one?

S.No	Hindi Statements	English Translation
1	pehle aisa hua tha, call pe bola ki 5000 ka coupon accept karo par khola toh pay dikha raha tha aur debit from me mera account no, tha toh pay toh matlab mai de raha hu toh nahi kiya	Earlier, something like this happened. They called and said to accept a ₹5000 coupon, but when I opened it, it was showing 'pay' and debited ₹5000 from my account. So, 'pay' means I am giving it, right? I didn't do it
2	Screenshare nahi karna chahiye tha Pin maang lete hai kuch log who nahi dena chahiye in case kabhi QR bhi galat hota hai	I shouldn't have shared my screens; some people ask for the PIN, which should not be given in case the QR code is also incorrect
3	Proof hona chahiye ki humne invest kiya hai. agar baad me mujhe kuch refund karna ho ki mujhe aur zyada din invest nahi karna hai toh I show the proof ki maine apke isme invest kiya tha toh aap mujhe wapas karo	There should be proof that we have invested. If later I need to refund something or I don't want to invest for more days, then I can show the proof that I had invested in this, and you should return it to me
4	pata nahi hai ki ek no. se alag alag account connect kar sakte hai	I don't know that we can link different accounts with the same number
5	Jisko paisa ka lalach hai woh fass jaega	Those who are greedy for money will get trapped
6	Jo padha likha hai woh nahi fase ga aur jo padha likha nahi jai woh jaldi se fas jaega	Those who are educated won't get trapped, and those who are uneducated will get trapped quickly
7	Badges toh hai, signal deta hai ki sahi hai ya galat hai	Badges are there, they signal whether it's right or wrong
8	jisko jaan pehchaan nhi hai usko nhi karenge	We won't pay someone we don't know
9	pehle verification fir pay ya nahi ka hona chahiye. Yes/ No fir Pay/ decline	First, there should be verification, then it should be a 'pay' or 'not.' Yes/No, then Pay/Decline
10	Dekhti ki sahi jagah me kar rahi hu aur kitne paise kat rhe exactly	I check if I am doing it in the right place and how much money is being deducted exactly
11	transaction history nahi hai, check karne k liye hona chahiye	There is no transaction history; it should be there to check
12	jaan pehchaan nhi hoga toh koi dega bhi toh lega nhi. wo kyu bhej rha hai	If there is no familiarity, even if someone gives, I won't take it and why is he sending it ?
13	Qr k jagah naam se pay karna chahiye. Qr unsafe hai	Instead of using QR codes, one should pay using the name. QR codes are unsafe
14	screen freeze wala achcha nahi hai, OK karne se kaha chala jaega nahi pata. Toh woh theek nahi hai. Kiss cheez karne k liye OK maang raha hai woh clear nahi hai	The screen freeze notification design is not nice. I will never know where I could be directed by clicking on OK. It is not clear
15	asal zindagi me fraud se bachne ke liye hum payment nhi karte	In real life, I would not make the payment to save myself from fraud.

Table 7: English Translation of partcipants' hindi quotations from our study.

E Translation of Hindi statements

Table 7 presents the original hindi quotations (in roman script) used in this work. We also added English translations.

F List of phrases queried on reddit

List of all the phrases queried on reddit: "upi frauds", "upi frauds in india", "upi scams", "olx upi scams", "olx scams", "amazon upi frauds", "payment frauds in india" and "india upi".

G Details of Key Functionalities and Interface Elements of UPI Apps

Table 9 details the six key functionalities of our investigated UPI apps. Table 8 details the categories of general nudges described by Franz et al. [45] and Table 3 shows the alignment of our four key nudges with Franz et al.'s framework.

H Nudges incorporated in UPI-Pay

Figure 2 presents the different nudge designs (including different) colored badges implemented in the UPI-Pay app.

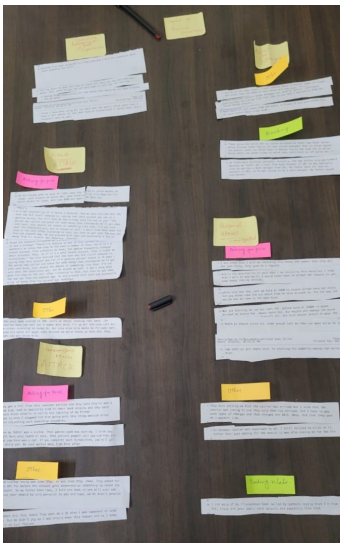


Figure 4: The qualitative coding process performed by two researchers

Category	Design Interventions
Education	Educational interventions
Training	Serious game, Embedded training, Mindfulness based training
Awareness-raising	Interactive warning, Passive warning
Design	Visual elements, Color Code, Highlighting, Customization, Redirect user's course of action

Table 8: Taxonomy of user-oriented phishing interventions

Functionality	Description	Apps with this feature
Send money	Sending amount by entering the receiver's UPI ID, account number or by scanning/uploading a QR code. Paytm and Phonepe also show a symbol with the receiver's name to signify whether the receiver is a verified app user.	All apps
Request Money	Request money from other UPI-app users by entering their UPI ID	Google Pay
Scan QR code and Pay	For paying an amount to the intended receiver. The QR codes can also be loaded from the gallery and shared with others for transactions.	All apps
Show transaction History	Show all past transactions up to three months.	All apps
Show user profile	Available as a profile icon. Shows the user information and generate QR code for a user	All apps
Show/Choose bank account	For users to choose from multiple bank account registered in the app during payment. Paytm and PhonePe allow choosing a bank account on the same interface as entering the payment amount; Google Pay shows a popup with the bank account option right after clicking the payment button.	All apps

Table 9: Six basic functionalities available in all UPI apps, uncovered by survey of UPI app functionalities.

Security Concerns	Trust	Need	Digital Literacy	Serious and observant	Outliers	Preferences
Rechecking every step	Trust in process	Urgency	Aware of UPI features	Actively thinking during transactions	Extreme orthodox concerns	Prefers instant assistance
Considers worst case or future scenarios	Trust in person	Vulnerabilities	Awareness of fraud	Alternative suggestion		Reluctancy
Observes details like notification, amount, account name	Trust in company		Awareness of various means of social media	Observant		
Privacy			Lack of Digital Literacy	Rechecks every step		
Some unusual security behaviours			Financial Awareness	FInd shortcomings of the desiign		
Expectation mismatch			Lack Of Device Familiarity	Initial Questions		
				Clear thinking		
				Situational Unawareness		
				Clarity		
				Curiosity		

Figure 5: The hierarchical themes uncovered by our affinity diagramming approach.

I Codebook

Figure 5 presents the hierarchy of themes from our open coding followed by affinity diagramming. Figure 4 presents a glimpse of the process performed by the 2 researchers. We have a total of seven themes and thirty sub-themes explaining the decision making process of UPI users.