A Platform for Uncovering Indian Users' Decision-Making Process in Unified Payment Interface (UPI) Apps

Kshitiz Sharma*
IIT Kharagpur

Nandini Bajaj*
IIT Kharagpur

Xinru Page
Brigham Young University

Mainack Mondal
IIT Kharagpur

Abstract

Online payment methods have gained enormous traction in India due to the launch of Unified Payment Interface (UPI), an API developed by the government-based identity National Payments Corporation of India (NPCI). UPI facilitates free and instant money transfers between users' bank accounts. Multiple financial apps use this API. However, fraudulent activities related to UPI have also increased and social phishing is a threat. Our goal is to develop UPI app interface elements that can help users avoid falling prey to social engineering attacks. In order to do so, we developed a UPI app simulator which provides a way to ethically test user interaction with various interface elements, without collecting or exposing their personal financial data. This paper demonstrates how our simulator can be used to understand UPI user decision-making processes, which will help us devise human-centered phishing prevention strategies.

1 Introduction

Indian citizens conducted financial transactions primarily via cash until 2016, when the Reserve Bank of India (RBI) launched the Unified Payment Interface (UPI) API to encourage its citizens to use electronic payment methods. UPI facilitates digital micro-payments at scale and empowers Indian users to transfer money quickly. It has a back-end architecture that allows easy integration and interoperability of new payment apps. This method of payment shows an enormous growth trajectory with the digital payments market in India valued at INR 1,638.49 trillion in FY 2019 and expected to reach INR 4,323.63 trillion by FY 2024 [7]. Currently, there are about 31 UPI payment apps and over 297 banks that enable transactions with those apps via UPI [9, 10].

However, with the rising popularity of UPI, attacks to defraud people using UPI have also increased. TrustCheckr, a fraud preemption platform, identified over 1 million frauds in just 15 months following January 2020, often resulting from fake accounts or social engineering [4]. Earlier work analyzed UPI-based payment apps to discover security vulnerabilities [8] and proposed protocol-level security improvements. However, it is becoming increasingly apparent that the security of UPI can be circumvented by misled humans. Thus, it is vital to understand people's decision-making processes that can leave them vulnerable to fraud.

While studying people's behaviors in real-life scenarios would be most informative for understanding their decision-making, prior work points out the ethical issues of attempting "Social Phishing" [5] through real-life attacks on participants. On the other hand, surveys and interviews rely on self-reflection and cannot capture insights that only occur in situ. It is important to observe users interacting with an actual UPI interface whose design can greatly shape their decision-making and reactions. Thus the key challenge we address in this work is: *How do we ethically uncover the decision-making process involved with using UPI apps?*

2 Background and Related Work

Prior research uncovered how fraudsters leverage social engineering techniques to manipulate people and let them divulge confidential information online [11]. Much of it draws on Robert Cialdini's principle of influence from the social sciences [2]. However, it is not clear how this manipulation is done through UPI apps. Prior security research for UPI-based payment apps primarily focused on protocol improvements [8]. Some relevant work has looked into utility of general default settings for leading to better security configurations [2].

However, there is no work so far on *how* the interface of UPI apps affects the decision-making process for Indian users. Faulty decision-making often leads to successful fraudulent transactions (as opposed to any secu-

*Both authors contributed equally to this work.

rity vulnerability of UPI protocol). So, there is a need for a detailed analysis of user perceptions of UPI apps and the various interface elements that are commonly used in these apps which affect these perceptions. Users' decision-making can be shaped by a combination of the interface, personal background, and context. Thus, creating a platform to understand and evaluate the impact of various interface elements on user decision-making is crucial to design against social phishing in UPI apps.

3 Methodology

In order to understand the user's low-level decision-making process, we need to observe them engaging in an UPI transaction. While procuring financial data from users' real-life interactions might give us ecologically valid data, there are huge ethical issues with manipulating people to investigate how they react to social phishing [5]. Thus, we explore an alternative approach to present realistic scenarios involving UPI transactions in a much more immersive way than could be accomplished through scenario-based surveys or interviews.

Our methodology involves simulating malicious and non-malicious UPI use cases that people experience in real life, but in a virtual, safe environment, that does not gather personal data nor cause a financial attack. To do this, we created a smartphone simulator and a dummy application that emulates the design of widely used real-life UPI applications. It is widely acknowledged that the design of app interfaces can overwhelmingly shape the decisions made by users [12]. Thus, researchers need to be able to test out various interface designs and see how they shape decision-making and behaviors. To easily and quickly test new UPI interface designs, the simulator application existed only on the interviewers' computers. Thus participants interacted without installing any tools, increasing the number of participants who could easily participate in the study. Participants interacted with our simulated UPI app via Zoom's remote control feature.

We developed the simulator using XCode [1]. The dummy UPI application (named UPI-Pay) is an emulation of real UPI apps with no real currency or financial record sharing involved. The design of UPI-Pay is motivated by existing popular UPI apps to maintain the look and feel of a UPI app for a regular user. It is built to include the features required to complete essential day-to-day UPI-related use cases, as described next.

The government sets the required baseline for transfer-related functionality that must be supported in a UPI app and thus API specs are provided by Nfinite (`https://nfinite.in`). Developers use these APIs, but can independently decide how to implement their user interface. We studied the NPCI guidelines and incorporated the interface design of features offered in the most popular UPI apps into our dummy UPI Application (UPI-Pay). This gave us confidence that our simulator would feel like a typical UPI app to the general Indian population. Our simulator has the following components:

Home Page: First page when UPI-Pay is opened. It has functionalities like "paying via scanning QR code", "paying using contact number", "requesting a payment" or simply "opening account details page".

Get My Balance Page: Accessed by clicking the user logo on the top right in the home page.

Payee Information and Transaction: Accessed by clicking one of the payee search results.

Transaction Views: Is the last step of any transaction. Consists of "Account selection view", "Pin Entering View" and "Transaction completion status view".

Payment Request View: Triggered by the requester externally and appears on home page.

Next, for a better illustration of our UPI simulator, we show a sequence of steps that the user would take in order to use one of the most common features—"Pay via contact no." (similar mechanisms are implemented for all other common UPI features).

Search Receiver (Fig. 1a): Users enter receivers' contact no. and choose the recipient from the presented options.

Enter Transaction Amount (Fig. 1b): The user enters the transaction amount and chooses bank account they want to pay from.

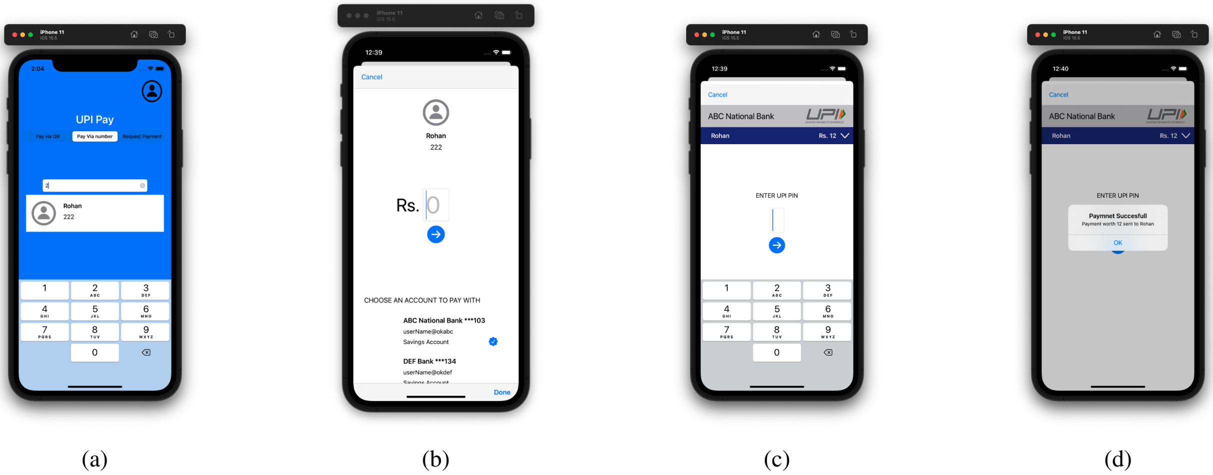
Enter Pin number (Fig. 1c): The user enters the UPI Pin which is pre-configured to be "0000" for the simulator.

See Completion status (Fig. 1d): The app alerts the user as to whether the transaction was successful or not, providing brief details of the transaction.

We further developed realistic scenarios where a user could use the simulator and decide whether to accept or send payment. By having users interact with a realistic and visual representation of the UPI app, we can observe how they react to and use the app in these real-life (both malicious and benign) scenarios. We found that enacting these scenarios through the simulator was important to evaluate the influence of the user interface elements which are key to shaping people's behaviors [3]. For this initial evaluation of the simulator, we chose to use interface elements that are common in UPI apps and examine if they indeed helped people avoid fraud.

3.1 Protocol

We developed an interview protocol using this simulator. For each interview, we first presented the participant



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

Figure 1: Steps followed by an user while paying via contact no: (a) Search Receiver (b) Enter Transaction Amount (c) Enter Pin number (d) See Completion status.

with scenarios involving a financial transaction and allowed them to use the app to make the transaction. Participants were asked to think aloud as they used the simulator so that we could understand their thoughts, beliefs, and concerns. After completing several scenarios (involving the most frequently used UPI features), we conducted a semi-structured interview to probe their past experiences having to do with UPI. We also debriefed them on whether each scenario was fraudulent and asked them to reflect on their decisions for each. The think-aloud design of the study allowed the interviewer to hear and capture the mental model of the subject, as well as capture erroneous assumptions. Each participant received Rs. 300 (approximately the average daily wage of an Indian worker) as compensation. To familiarize participants with the simulator, participants were encouraged to try out the different features of UPI-Pay before the interview started. Each interview lasted approximately 15 minutes. In this proof-of-concept work, we present results from two participant sessions. Our protocol is examined and approved by the IRB of BYU.

3.2 Limitations

Our methodology is not without limitations—it is based on a simulator and we did not launch real attacks. It is possible that our use of a desktop environment rather than a more familiar smartphone environment might slow the users (e.g., due to using a mouse rather than a touchscreen). We also did not use participants' actual bank accounts and transfer money for ethical reasons, perhaps leading participants to be less vigilant. However, the think-aloud technique still allowed us to capture their valid mental models as has been done in prior work [6]. Furthermore, participants might attribute characteristics of malicious scenarios (e.g., a very different amount to transfer than agreed upon) to researcher or simulator error. However, we explicitly asked participants why they took decisions about transactions in our protocol and used the think-aloud responses to clarify such doubts. Finally, we randomized the scenarios to avoid biases in the user decisions and focused on uncovering user perceptions and mental models via our study rather than just capturing behavior. Thus we believe that our study uncovered important factors in decision-making.

4 Results

The scenarios presented to our two participants involved payment and request transactions via contact number and QR code. To test whether participants would pay attention to visual cues presented in the UPI interface, one of the scenarios involved minor discrepancies between the money requested and the amount showing up on the screen.

4.1 Fraudulent Scenario

In this study, we designed a scenario: the UPI-Pay user receives a money request from a shopkeeper who says that he will charge Rs. 300, but sends a request of Rs. 1,500 on UPI-Pay. On the simulator's interface the message associated with the request said "Pay Rs. 300". However, the final payment amount in bold is Rs. 1,500 (Figure 2).

The scenario was tested with two participants using our protocol. Table 1 shows that both the participants overlooked the information that would have clued them

	Response	Transaction Status
Participant 1	They ignored the mismatch in the amount requested and encoded it in the payment request.	Successful
Participant 2	The participant ignored the notification popup that reiterated the amount requested and made the fraudulent payment in haste.	Successful

Table 1: Results from the Pilot Interviews

into the incorrect amount and, as a result, paid excessively.

In fact, to explain their decision, Participant 1 mentioned, *“did not know that payment can be requested via the app and accepted instantly”*, showing a lack of attentiveness as well as awareness on the users’ end that makes them vulnerable to fraudulent attacks. The interface design interventions, e.g., written in bold did not help in this case.

4.2 Concerning Inattentiveness of Users

Developers often tend to create apps with the best possible features and functionalities, but fail to think about the user’s perspective. It is vital to note that for the user to be able to benefit from the security features of an app, they need to first notice those features. Developers need to pull the user’s focus to the relevant information they are conveying in the app. This simulator can be used to test out new designs aimed at bringing the user’s focus to the relevant information. Prior work shows that a major enabler of fraudulent attacks on users is overlooking key details while using a given piece of technology [12].

Being able to focus on the details of the app interface is crucial for UPI users. Technologies such as payment apps require particular attention from the user since they can have major financial consequences. The inattentiveness of the participants was clearly visible during the interviews. While participants were attentive at the onset of a scenario, they gradually became less vigilant and ignored important notifications and verification nudges. By having them walk through a complete scenario of engaging in a UPI transaction from start to finish, we were able to see how this transpired. Whereas if we just showed them that screen in a survey, or asked about it in an interview, we would not have been able to observe this temporal-dependent behavior.

While this gives us initial insight into a possible reason to succumb to fraud, further research needs to look into real-world social phishing and determine if users would have the same inattentiveness if it were their own finances involved. Thus, our simulated UPI approach allows us to take a step toward identifying potential issues that can be further investigated.

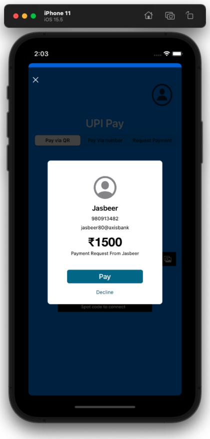


Figure 2: Fraudulent Payment Request

5 Conclusion

Initial evaluation of our simulator using a think-aloud protocol indicates that our approach can be used to uncover issues with the user interface, and people’s attitudes towards UPI apps. This approach can be used across different scenarios to test how people would use the app in different contexts.

We observed that there are features like notifications that are known to have major security importance, but was more often than not ignored by the users. Similarly, the amount validation page that includes the sender and receiver’s details along with the transaction amount and a message, was commonly accepted in haste. These features that allow a second verification before acceptance are observed to be treated as superfluous steps by the participants, leading them to fall for fraudulent transactions on the UPI app. This inattentiveness is more pronounced in later transaction steps.

In order to get a deeper insight into the mental models of UPI users in a variety of scenarios, we intend to conduct extensive interviews. These interviews will be targeted at UPI users belonging to different socio-economic and educational backgrounds. We will enhance the interview protocol by designing different scenarios that cover prominent usages and transactions made on the UPI-Pay app. Overall we are motivated to gain deeper insight into the users’ response to the scenarios through a variety of user interface designs and attack models to understand the factors that influence the decisions made by UPI users.

References

[1] APPLE. Xcode. `https://developer.apple.com/xcode/`.

[2] CRANOR, L. F. A Framework for Reasoning about the Human in the Loop. In *Proceedings of the 1st Conference on Usability, Psychology, and Security* (2008).

[3] FOGG, B. *Persuasive Technology: Using Computers to Change What We Think and Do (Interactive Technologies)*. Morgan Kaufmann Publishers, 2003.

[4] IANS. Attention! UPI, payments frauds soar high in eastern Indian states: Report. https://www.indiatvnews.com/business/news-upi-payments-frauds-soar-high-in-eastern-indian-states-report-701790, May 2021.

[5] JAGATIC, T. N., JOHNSON, N. A., JAKOBSSON, M., AND MENCZER, F. Social phishing. *Commun. ACM 50*, 10 (oct 2007), 94–100.

[6] JAKOBSSON, M., TSOW, A., SHAH, A., BLEVIS, E., AND LIM, Y.-K. What instills trust? a qualitative study of phishing. In *Financial Cryptography and Data Security* (2007), pp. 356–361.

[7] KPMG. Impact of COVID-19 on digital payments in India. `https://assets.kpmg/content/dam/kpmg/in/pdf/2020/08/impacting-digital-payments-in-india.pdf`, August 2020.

[8] KUMAR, R., KISHORE, S., LU, H., AND PRAKASH, A. *Security Analysis of Unified Payments Interface and Payment Apps in India*. 2020.

[9] NPCI. UPI live members. `https://www.npci.org.in/what-we-do/upi/live-members`, 2022.

[10] NPCI. UPI third party apps. `https://www.npci.org.in/what-we-do/upi/3rd-party-apps`, 2022.

[11] SCHNEIER, B. *Secrets and Lies: Digital Security in a Networked World*. John Wiley and Sons, 2000.

[12] SOMANCHI, S., AND TELANG, R. Security, fraudulent transactions and customer loyalty: A field study. In *ICIS* (2016).