

# Understanding Social Engineering and it's impact on Merchant basedUPI frauds.

Simran Jain

University of Mumbai Institute of Distance & Open Learning (IDOL)  
Information Technology, University of Mumbai

\*\*\*

**Abstract** - Social engineering cyberattacks are becoming an increasing concern in the field of cybersecurity. This attack uses psychological techniques to trick people into disclosing sensitive information or performing actions that could compromise the integrity of the system. In recent decades, social engineering attacks have become more sophisticated, making it harder for individuals and organizations to detect and prevent them. With the increase in UPI based payment usage, there is an exponential growth in UPI based frauds primarily by using Social Engineering Techniques. Considering this, our research was conducted to understand how these social engineering attacks are executed by malicious party by keeping merchant users of UPI as a prime target. This was conducted by taking real examples of OR code manipulation using watering hole concept of Social Engineering. We also discuss how these social engineering attacks could be prevented and UPI based payments could be made safer. This is one of the studies in India to comprehensively understand fraud and scams in UPI based payment models focusing majorly on social engineering-based attacks on merchant users of UPI-based payment apps and empirically investigate factors driving the increasing frauds in this adopted model of payment.

**Key Words:** Social Engineering, UPI, UPI Frauds, UPI mechanism

## 1.INTRODUCTION

Social engineering is a type of attack that involves manipulating people to obtain information or resources. It is a kind of psychological tampering used to gain unauthorized access to private data such as passwords, credit card numbers, or other personally identifiable information. Social engineering attacks are becoming more frequent since they're simple to carry out and can be difficult to detect. Refer Fig-1 to understand the Social Engineering Lifecycle.

UPI a term that stands for Unified Payments interface. UPI is a real-time online payments system developed and maintained by the National Payments Corporation of India. Its primary working protocol is that it allows users to transfer funds between bank accounts instantly using an active mobile device through a payment's application. According to Yash Madwana et.[1], Dominant working

features of UPI is that it is a simple and secure method of transferring UPI money without the need for entering bank details or IFSC codes. Users are assigned a virtual ID (called UPI ID) which is linked to their bank account and can be used to make transactions.

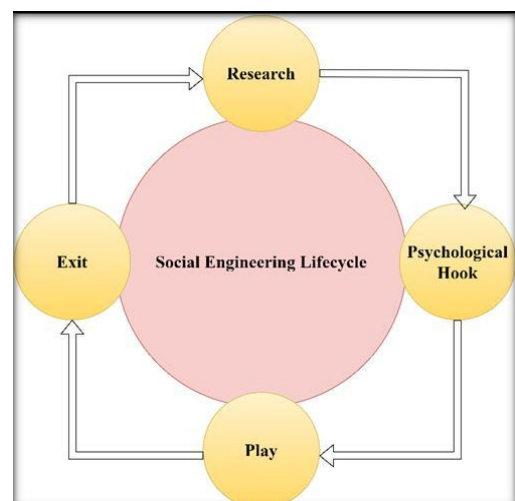


Fig-1: Social Engineering Lifecycle

### 1.1 Banking based social engineering tactics.

This UPI scamming technique using smart social engineering skills involves an email or text message that appears to be from a legitimate bank, asking the recipient to click on a link to log in, leads to a fake website where cybercriminals can use this information to access the victim's real bank account and steal money or sensitive information, is a common example of banking-based phishing.[2]

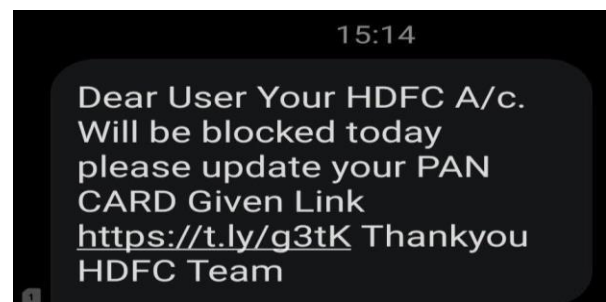


Fig-2: Fraud phishing message disguised as a bank SMS.

### 1.2 Phishing of Bank Websites & Emails

Cybercriminals frequently use tactics such as creating fake email addresses that closely resemble the bank's official email address, websites or including the bank's logo and branding in the message to make the phishing message or webpage appear more legitimate.



Fig-3: A legitimate bank website form.

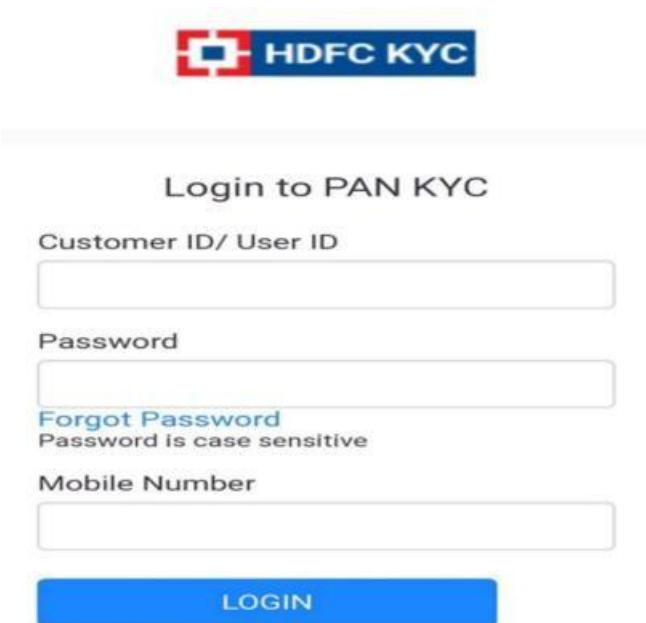


Fig-4: A fraudster developed fake website form.

Individuals must be vigilant and cautious when receiving unsolicited emails or communications from banks or financial institutions. Individuals should never click on

links or download attachments from unsolicited emails or text messages and should always verify the authenticity of any requests for personal or financial information to avoid falling victim to banking-based phishing attacks. Individuals should also use strong, unique passwords for their online accounts and enable two-factor authentication whenever possible.

### 2. UPI & IT'S WORKING MECHANISM

The low-level working of Unified Payments Interface payments involves various components and protocols such as HTTP, SSL, TLS, and 2FA (Two-Factor Authentication) that work in unison to ensure the secure and error free transfer of funds between banks. An overview of steps involved is User Registration where the user is registered and the bank account is securely verified and linked to the user's UPI account, setting up a UPI pin for enabling transactions. Similar process is followed for a merchant account willing to setup their UPI account via QR code scanner. Further, a Virtual Payment Address (VPA) is generated by a user's or merchant's bank which is a unique identifier linked to their bank account. Payment Initiation takes place from a consumer side via their UPI application by entering merchant VPA or by scanning their QR code which further queries a request with order and payment details to the UPI interface. A payment process is initiated with generation of payment details. Upon these processes, the QR code scan process is initiated. This enables direct payment service generation from user UPI application to the UPI interface via PSP (Payment service provider). Upon further verification of payment from user. The NPCI switch receives the payment request and opts to check for user account balance to ensure sufficient funds, if sufficient funds are verified, the switch forwards the user request to the bank for authentication. Authentication step enables the bank account to send an authentication request to the user's mobile device and prompts them to input their UPI pin. Further an authorization check takes place where in the linked bank account authorizes the payment and relays the process back to the NPCI switch[3]. Further, the UPI initiates a status update thread via webhook and provides it directly to the merchant. Final step is generation of update query on the user side which marks the end of a UPI payment cycle between user and merchant. Low level working of the payment transaction can be referred in Fig-5.

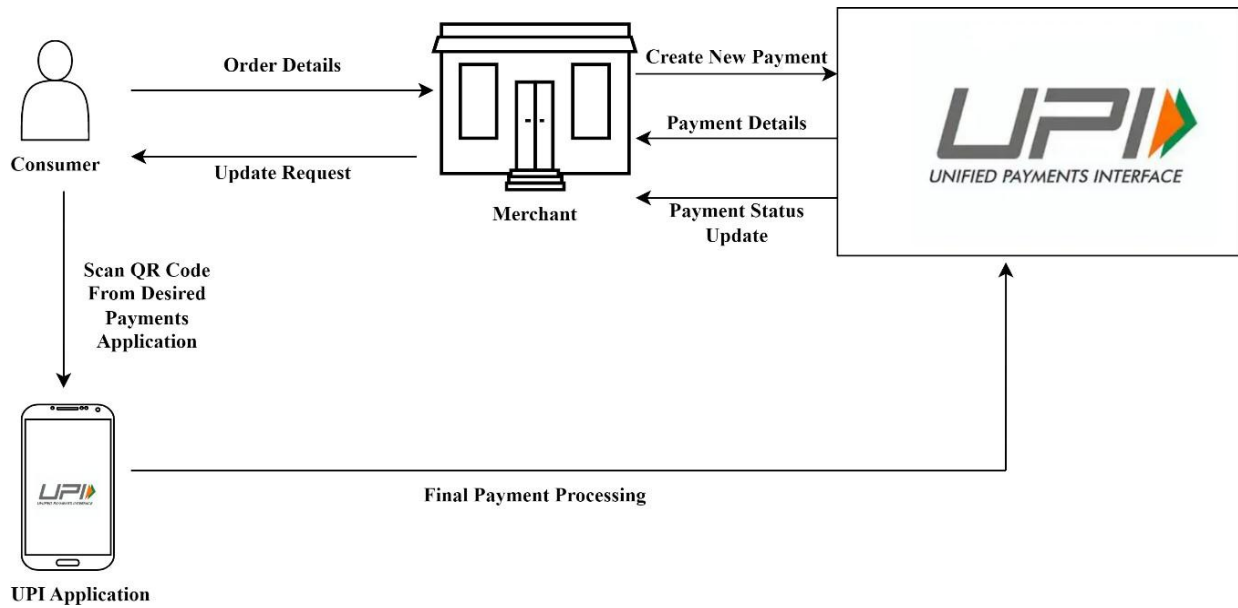


Fig-5: Low level working of a UPI payment transaction

### 2.1 How UPI frauds occur via social engineering

UPI (Unified Payments Interface) frauds using social engineering are becoming a common trend now due to increase in UPI users in the country. Frauds typically involve a fraudster tricking a victim or merchant using UPI QR codes into providing their UPI credentials, such as their UPI PIN or UPI ID, through some form of social manipulation. The social engineering-based attack to give rise to UPI frauds in on high increase day by day. A normal working of a UPI based social engineering fraud includes an attacker to lure the victims into visiting the fake site or downloading the fake app by sending them phishing emails or social media messages. Once the victims access the fake UPI payment app or website, the attackers can steal their UPI PIN, password, or other sensitive information. The attackers can also use the fake app or website to initiate fraudulent transactions from the victims' bank accounts.

One trend in UPI frauds using social engineering is targeted towards merchant accounts opting for UPI payments using QR code which is what our research paper focuses on. A simple working of this technique is that a user scans the QR code implanted by a merchant and instantly gets account details of the user after which the user can opt to enter the amount on their respective UPI application and proceed to pay the merchant. As the number of merchants opting for UPI based payments is increasing, so is the commensurate amount of UPI based frauds with these merchants.



Fig-6: UPI id of a normal user

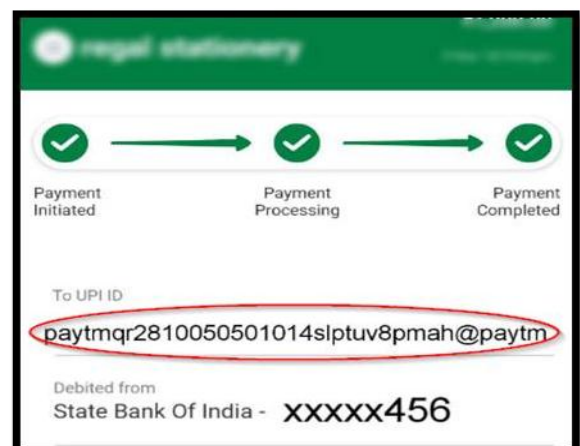


Fig-7: UPI id of a merchant user

## 2.2 Watering Hole Social Engineering Attack

Our primary focus is to analyze the trending social engineering attack called Watering hole attack where the primary targets are merchants. This social engineering-based attack works as follows:

1. The attacker locates the merchant shop and figures out the UPI Scanner that the merchant is using.
2. Next, through a series of manipulation, often pretending to be a technician from UPI payments company, they get hold of the QR scanner.
3. The attacker then opts to replicate the QR code scanner exactly as the shop owner's scanner, only difference would be that the attacker would replace the merchant's QR code with their own QR code.
4. This shall enable the payments directed for the merchant to be redirected to the attackers account instead.
5. One of the points to be noted for why this scam is not easily detected by Merchants is the UPI name that the merchant gets. It is a series of random character set which is usually never readable and can't be memorised by a naïve user. Refer fig 7 for the UPI id that has random characters generated to maintain uniqueness.
6. The attacker takes advantage of this loophole to successfully implement the social engineering attack and thereby scamming the merchant opting for UPI based payments.

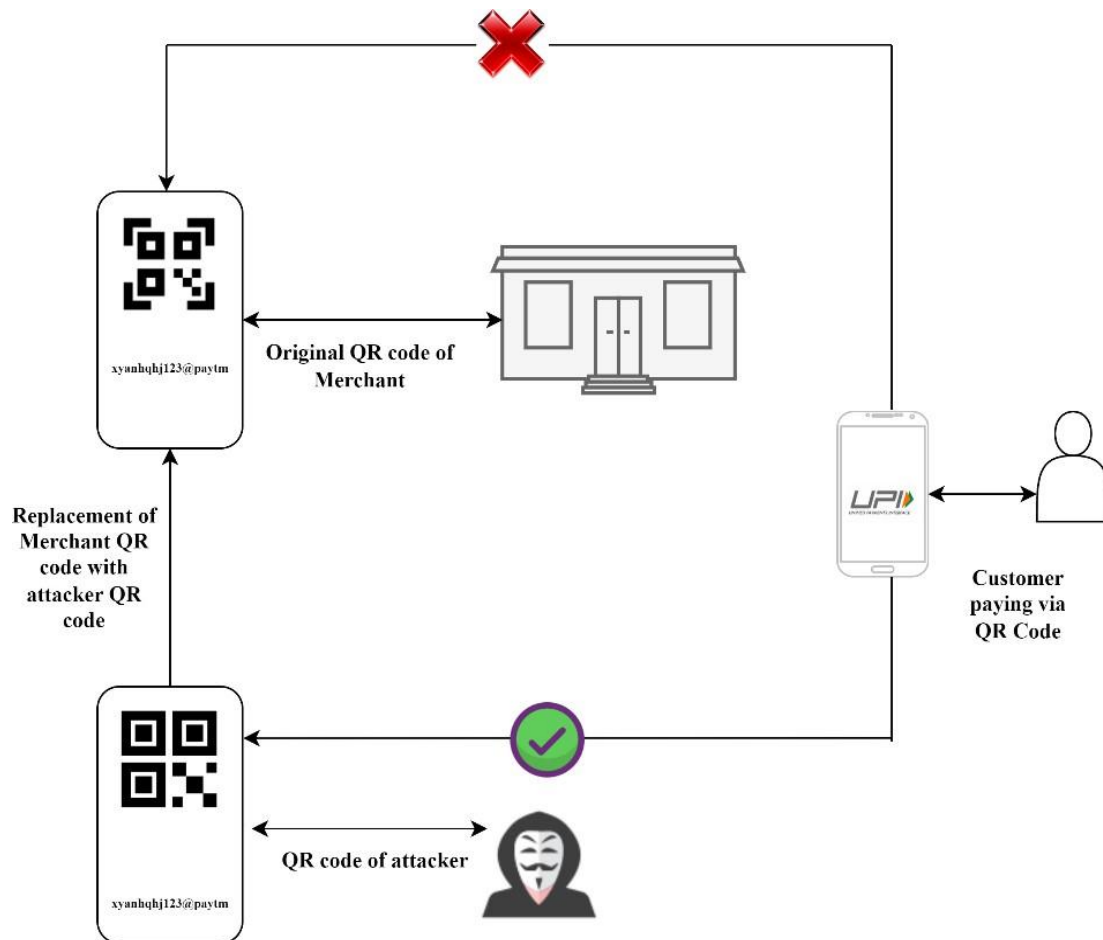


Fig-8: Flow Diagram explaining QR code manipulation using Social Engineering



### 2.3 Defense against such social engineering attacks

To combat social engineering-based UPI fraud, a fusion of education, awareness, and technological solutions is a mandatory. A few methodologies that could be followed are:

**1. Education and awareness:** A form of combating could be conducting educational seminars, awareness camps, and educational camps for merchants for safer usage of UPI application daily. This would enable the merchants to be vigilant and aware users of UPI based payment applications.

**2. Two-factor authentication:** An added layer of security in the form of 2FA can be implied by the user which will give an extra step of security in form of authentication and will ensure that the added layer works to provide security to the merchant account and prevent any fraudulent transfers.

**3. Manual Verification:** One of the loopholes that a hacker takes advantage of using social engineering is the random character generation upon payment, this could be fraudulent transfer and can take advantage of the merchant's naivety. To ensure this doesn't happen, the merchant must ensure manual verification of the payment received from the consumer, if any suspicious activity is detected they should immediately raise an issue at the UPI help center.

**4. Collaboration & Use of technology:** Collaboration between individuals, merchant organizations, and law enforcement agencies can help prevent and detect social engineering-based UPI frauds. This includes sharing information about new threats and collaborating on strategies to identify and prevent these types of frauds. Merchants can opt to use various technological solutions such as Paytm soundbox, which upon successful transaction, recites a full audio message of the amount received thereby making the merchant aware and verify the transaction that took place.

Individuals and organizations can reduce their risk of falling victim to social engineering-based UPI frauds and protect themselves from financial losses and other negative consequences by implementing these defense strategies.

### 3. CONCLUSION

In recent decades, UPI-based social engineering fraud has become a growing concern. As more people depend on UPI-based payment systems for financial transactions, cybercriminals are developing new methods to exploit vulnerabilities in these systems to commit fraud.

Additionally, UPI-based social engineering frauds can have serious financial and personal consequences for victims. Private citizens must be aware of the risks and take precautions, such as verifying the authenticity of payment requests and keeping their personal information secure. Organizations and financial institutions should also take an immediate measure to prevent and detect social engineering fraud, such as monitoring for suspicious activity and providing employees and customers with education and training.

UPI-based social engineering cases of fraud are likely to remain a severe risk as the digital economy continues to grow. Individuals and organizations, on the other hand, can minimize the likelihood of falling victim to these types of scams by remaining vigilant and taking proactive measures.

### REFERENCES

- [1] Yash Madwanna, Mayur Khadse, B R Chandavarkar, "Security Issues of Unified Payments Interface and Challenges: Case Study", *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, pp.150-154, 2021.
- [2] IANS. Attention! UPI, payments frauds soar high in eastern Indian states: Report. <https://www.indiatvnews.com/business/news-upi-paymentsfrauds-soar-high-in-eastern-indian-states-report-701790>, May 2021.
- [3] NPCI. UPI live members. <https://www.npci.org.in/what-we-do/upi/live-members>, 2022.
- [4] NPCI. UPI third party apps. <https://www.npci.org.in/what-we-do/upi/3rd-party-apps>, 2022.
- [5] Aburrous, M., Hossain, M., Dahal, K., & Thabtah, F. (2010). Intelligent phishing detection system for e-banking using fuzzy data mining. *Expert Systems with Applications*, 37(12), 7913-7921. <https://doi.org/10.1016/j.eswa.2010.04.044>
- [6] Gupta, Nakul , Jhamb, Dharmender, "How India can develop it's fraud prevention model Journal of Payments Strategy & Systems, Volume 14/Number3 /Autumn/Fall 2020, pp. 237-255(19)
- [7] <https://www.npci.org.in/>
- [8] Kumar, A., Choudhary, R. K., Mishra, S. K., Kar, S. K., & Bansal, R. (2022). THE GROWTH TRAJECTORY OF UPI-BASED MOBILE PAYMENTS IN INDIA: ENABLERS AND INHIBITORS. *Indian Journal of Finance and Banking*, 11(1), 45-59. <https://doi.org/10.46281/ijfb.v11i1.1855>.

- [9] Zulkurnain, A.U.; Hamidy, A.K.B.; Husain, A.B.; Chizari, H. Social engineering attack mitigation. *Int. J. Math. Comput. Sci.* **2015**, *1*, 188–198.
- [10] Parekh, S.; Parikh, D.; Kotak, S.; Sankhe, S. A new method for detection of phishing websites: Url detection. In Proceedings of the Second IEEE International Conference on Inventive Communication and Computational Technologies, Coimbatore, India, 20–21 April 2018; pp. 949–952.
- [11] Charvi Vij, Shruti Keshari, "Study on Lexical Analysis of Malicious URLs using Machine Learning", *2022 Fifth International Conference on Computational Intelligence and Communication Technologies (CCICT)*, pp.120-127, 2022.