International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 14 Issue 02, February -2024,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

The Cyber security Conundrum: Unraveling UPI Scams in India

Venkatesh H. Assistant Professor, Department of Computer Applications, Presidency College, Bengaluru-560024

Salman Rehim, Department of Computer Applications, Presidency College, Bengaluru-560024

Abstract – From scaling micro-transactions to making digital payments accessible to all, UPI serves as the paramount. UPI has surpassed all other competing digital payment methods in a remarkably brief temporal interval. However, there are also some shortcomings and limitations associated with this expansion. An analysis and comprehensive review of the modus operandi of the fraudulent activities linked to the Unified Payments Interface UPI in the Indian domain will be carried out in this manuscript. This article provides elucidation into the remedial measures aimed at mitigating the impact of these scams to strengthen the integrity and effectiveness of UPI.

Keywords: upi scams, rbi, npci, types of scams, prevention

1. Introduction

Unified Payments Interface, often referred to by its abbreviation "UPI", is a digital payment platform introduced by the NPCI (National Payments Corporation of India) in April 2016. In accordance with the Payment and Settlement Systems Act of 2007, the Reserve Bank of India (RBI) along with the

Indian Banks Association (IBA) started an initiative to create an organization with the goal of building a strong payment and settlement system for the country and named it NPCI [1]. After the retraction of old currency notes, the government has been promoting digital payments through UPI to make the vision of Digital India a reality. Since its launch UPI has been on the rise, constantly overtaking other digital payment platforms such as digital wallets. UPI enables users to make tax-free and instant transactions between bank accounts directly with the use of a Virtual Payment Address (VPA) or Phone Number without revealing the bank account details. While other sectors were badly affected during the COVID pandemic, UPI experienced a boost in the number of users as more and more people switched to cashless methods. According to NPCI, there was a rise of approximately 48% in transaction volume and about 1600% in the amount transferred from 2019 to 2020, from 2020 to 2021, there was a further increase of around 64% in transaction volume and approximately 52% in the amount transferred [2]. As of January 2024, 550 banks are live on UPI with the volume of transactions at 12,203.02 million.

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 14 Issue 02, February -2024,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

Month	Banks live on UPI	Volume (in Mn)	Value (in Cr.)
Jan'24	550	12,203.02	18,41,083.97
Dec'23	522	12,020.23	18,22,949.42
Nov'23	516	11,235.29	17,39,740.61
Oct'23	505	11,408.79	17,15,768.34
Sep'23	492	10,555.69	15,79,133.18
Aug-23	484	10,586.02	15,76,536.56
Jul-23	473	9,964.61	15,33,645.20
Jun-23	458	9,335.06	14,75,464.27
May-23	445	9,415.19	14,89,145.44
Apr-23	414	8,898.14	14,07,007.55

"*Summary of UPI Activity from April 2023 to January 2024"*

With large-scale digitization and advancements of technology even scammers and hackers are finding new ways to break in. As many as 14,483 frauds were reported involving an amount of Rs 2,642 crore in the first half of the current financial year, as compared to 5,396 cases (Rs 17,685 crore) in the same period a year ago [3]. With such a large user base, digital scams are more likely to happen. Despite the improvements in UPI 2.0 compared to the drawbacks and security issues of UPI 1.0, criminals continue to exploit people. According to a report from Forbes, preloaded spyware may be found in certain brand-new phones, making it easy for the owner's information to be disclosed [4]. In 2021 the Reserve Bank of India issued directions called Digital Payment Security Control to set up a robust governing structure [5]. Social Engineering, Phishing and Sim cloning are some tactics being used by criminals to commit fraud. When these platforms were seldom utilized at all in 2017, a glitch in the Unified Payment Interface program led to the removal of 25 crore rupees from the Bank of Maharashtra, which was then approved by the National Payment Corporation of India [6]. To

educate people more about cybersecurity The Government of India has launched courses at UG and PG level [7]. We will learn more about recent scams related to UPI payments in this paper and how to prevent these scams.

2. Acronyms

In the course of our discussion on UPI scams, let us familiarize ourselves with the key acronyms that frequently appear in this domain. Some of the primary acronyms you will encounter in our exploration of UPI scams are given below:

UPI: Unified Payments Interface

OTP: One-Time Password

MPIN: Mobile Personal Identification Number

NPCI: National Payments Corporation of India

KYC: Know Your Customer

VPA: Virtual Payment Address

PSP: Payment Service Provider

QR Code: Quick Response code

SIM: Subscriber Identity Module

APK: Android Package

BHIM: Bharat Interface for Money

AI: Artificial Intelligence

NLP: Natural Language Processing

ML: Machine Learning

3. Working of UPI

Now, we delve into the fundamental workings of UPI. This will provide insight into its seamless functionality and will also shed light on the vulnerabilities that may be exploited by malicious individuals or groups.

UPI simplifies the money transfer process between individuals and businesses by allowing individuals to shop online, pay for utilities and shop in stores using QR codes, VPAs or UPI-registered mobile numbers.

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 14 Issue 02, February -2024,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

Customers use their UPI-enabled apps to initiate transactions and enter the details and amount of the recipient with an optional note. The customer's app forwards the transaction request to the payment service provider of his choice. PSP acts as an intermediary in the transaction process and forwards the query to NPCI to monitor UPI transactions. The issuing bank then verifies the correctness of the transaction, the balance and the credentials of the customer authorizes the transaction and creates a digital signature for security once approved.

For verification and remittance, PSP shares the sender's bank details with the UPI system. NPCI verifies the sender's account details, account balance and availability of funds. NPCI initiates the deduction of funds from the sender's account if funds are available. The receiving bank receives the transaction amount and credits it to the beneficiary's account. The UPI server sends a response to the customer's application confirming a successful transaction and providing a reference ID.

For payment requests, the sender can accept and complete the payment when the recipient issues a payment request. In this method, the recipient controls the initiation and completion of the transaction, which ensures the safe and authorized retrieval of funds.

To initiate the transaction, The recipient creates the requested information through their UPI-enabled application request. The payment request passes through the recipient's application to NPCI, which indicates the payer's intention to withdraw the amount. The payment request then reaches the creditor's bank, which then forwards it to the debtor's bank through NPCI. The merchant prepares a payment request for the customer's account. The merchant's bank sends the request to the customer's bank through NPCI.

The customer's bank verifies the request, account details and free balance.

The bank then accepts the transaction and confirms it with NPCI if the account has sufficient funds. The customer's bank transfers the requested amount to the creditor's bank and completes the transaction.

This encapsulates the fundamental mechanism underlying UPI transactions, providing a brief overview of how a transaction or a payment request takes place.

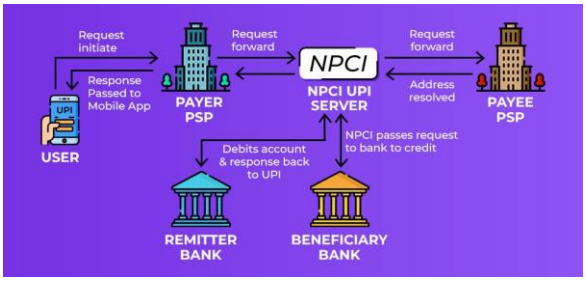

Fig 1"Working of UPI Diagram"

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 14 Issue 02, February -2024,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

4. Types of Scams

As we navigate the landscape of UPI, it is necessary to look into the diverse array of scams that have emerged within this digital ecosystem. This section aims to categorize the different types of scams plaguing the UPI platform. Now we will explore some of the common UPI scams that take place.

4.1 Phishing

Phishing Attacks happen when scammers deceive people into divulging their UPI credentials by sending false emails, messages or web pages which cause victims to unintentionally disclose sensitive information like passwords or PINs. Scammers also make up fake QR codes and offer them to others to scan. Unauthorized transactions could be initiated which leads users into scanning harmful QR codes ultimately causing them to transfer money without realizing it.

4.2 SIM Swap Fraud

SIM Swap Fraud involves deceiving the mobile service provider into moving the victim's phone number to a new SIM card in an effort to obtain control of the number. The fraudster can obtain OTPs and take over the UPI account once they have access to the victim's phone number.

4.3 Malware

Malware-based attacks occur when malicious software such as harmful APKs are installed on the user's device which compromises the security of UPI transactions. Sensitive data can be obtained by malware.

4.4 Vishing

Vishing, also known as voice phishing, is when scammers call someone posing as representatives of reputable companies like banks or UPI providers to instill a sense of urgency in order to obtain sensitive information.

4.5 Social Engineering

Social Engineering Attacks occur through psychological manipulation where attackers coerce victims into willingly divulging their UPI credentials. Techniques such as impersonation, building trust or exploiting personal information are often carried out.

4.6 Fraudulent Apps

Fraudulent mobile applications that are designed to steal user information imitate legitimate UPI apps and can cause users to unknowingly download and use these fake apps which then leads to unauthorized transactions.

4.7 Link Fraud

Payment Link Fraud is a scam where scammers send deceptive payment links to users prompting them to click and make a payment which may lead to fake websites that mimic official payment pages which results in financial losses for the victims.

5. Vulnerabilities of UPI Users:

This section offers an understanding of potential challenges that can lead users to be victims of UPI fraud. We can explore prevalent vulnerabilities faced by UPI users.

5.1 Weak Credentials

Users with weak or easily guessable passwords are vulnerable to unauthorized access that may expose accounts to brute-force attacks.

5.2 Device Security

Compromised devices infected with malware or other malicious software can lead to the theft of UPI credentials which can compromise the security of transactions.

5.3 Insecure Wi-Fi Networks

Using UPI on unsecured/public Wi-Fi networks can expose users to man-in-the-middle attacks where attackers intercept and manipulate data transmitted between the user and the UPI service.

5.4 Lack of User Awareness

Users who are not adequately informed about security best practices may fall prey to social engineering tactics like providing sensitive information to fake customer support agents.

5.5 QR Code Manipulation

QR codes used for transactions can be manipulated by attackers which will lead users to scan fraudulent codes and make unintended payments.

5.6 Misuse of Biometric Data

UPI apps often use biometric authentication. It can lead to unauthorized access if the biometric data is compromised, either through device-level security issues or attacks on the authentication process.

5.7 Social Engineering

Attackers can exploit human psychology to trick individuals into divulging sensitive information. Common tactics include impersonation, building trust and creating a sense of urgency to manipulate users.

Nowadays, AI too has been involved in UPI scams. AI can let scammers personalize messages and automate phishing. Convincing deep fakes and chatbots are also used to cheat others. Some countermeasures would be to provide cybersecurity education, vigilant communication practices and advanced AI-driven security solutions.

5.8 Security of Third-Party Apps

Users might use third-party apps that claim to provide additional features or services related to UPI which may have security vulnerabilities or may be malicious that can put user information at risk.

6. Recent UPI Scams

Let us examine some real-world scenarios to draw meaningful conclusions and to have a broader understanding of how some common UPI scams take place. Three cases are provided below.

6.1 Case Study 1:

In February 2024, four men, including three representatives of private banks, were taken into custody in Gurgaon after deceiving customers into making fraudulent payments via UPI.

Police commented that the victim got a call from a scammer pretending to be a friend, telling him that his son had been admitted to the hospital and was requesting Rs 10,000 to cover the costs. After being provided with a UPI ID, the complainant was instructed to transfer the money. Later on, it came to light that he had been tricked into sending the money to scammers [11].

The scammers here used emotional manipulation to exploit individuals. Verifying the information by directly contacting the affected or trusted family members is key. Avoiding

sending money immediately, asking specific questions to confirm identity and independently verifying hospital details would be the best choice.

6.2 Case Study 2:

In January 2024, A woman managed to thwart a potential UPI scam after receiving a call from an imposter claiming to be associated with LIC transactions. She was approached by a scammer who allegedly received her number from her father. The caller stated that because her father did not use the virtual mode of payment, he was forced to give the □ 25,000 LIC money to her instead of her father. The user consented to assist, not yet suspecting malicious play. The scammer quickly went through a series of transactions during the call, transferring money in real-time and putting pressure on the victim to validate the receipts.

But when the customer got □ 50,000 instead of the supposed □ 5,000, things became suspicious when the scammer tried to take advantage of this "mistake" by demanding □ 45,000 back.

Realizing the attempt to manipulate her, the user immediately became skeptical. The user claimed to only have received text messages but no money on her UPI apps. The scammer pressurizes her to send the money regardless. This led her to hesitate and tell the scammer that she needed to consult her father to verify the same [12].

Scammers use different pressurizing tactics to steal from victims. The pressure put by the scammer here is a manipulative strategy aimed at coercing individuals into making impulsive decisions, hindering their ability to think rationally. Common tactics of pressurizing include threatening consequences, claiming emergencies, or feigning authority. Individuals must recognize these pressure tactics, stay calm, and verify information independently before succumbing to such demands. Education and awareness about these tactics are key to empowering individuals to resist coercion and protect themselves from scams.

6.3 Case Study 3:

A man in Lucknow was scammed out of Rs 45,000 by a cybercriminal using AI. This was accomplished by using artificial intelligence to mimic the voice of his relative. Kartikeya, the victim, was duped into paying Rs 90,000 to a person he knew. In agreement, Kartikeya moved Rs. 45,000 out of his account. But he got an SMS saying that his account had been credited with the money four times.

Kartikeya reported that an unknown caller called his mobile phone. The caller identified himself as his maternal uncle and claimed that while he was paying Rs 90,000 to a known individual, his UPI was not fully completing the transfer of the funds. Kartikeya complied with his request and moved Rs. 45,000 from his account. After some time, the bank sent him an SMS informing him that his account had been credited with Rs 10,000, Rs 10,000, Rs

30,000, and Rs 40,000 four times. Kartikeya thought that the money had reached his account, but after checking out, he did not find the money.

Several transactions failed, and the transfer of only Rs 44,500 could have been possible fortunately for the victim [13].

UPI scammers leveraging artificial intelligence pose an escalated threat due to the technology's ability to personalize and automate attacks. AI can create convincing phishing messages, deep fakes, and chatbots that mimic trusted individuals which makes scams more sophisticated and harder to detect. The use of AI in social engineering exploits human vulnerabilities. Stringent authentication measures and advanced technologies are important to counter evolving threats.

Some common UPI scam scenarios are given below:

6.4 Scam 1:

This is a scam where the scammer requests the victim to send back money by claiming that it was sent by mistake. The scammer sends a message impersonating official bank messages that informs customers about money that has been credited to their account. The victim then sends the amount mentioned in the fraudulent message to the scammer out of their UPI account. Such a situation can be avoided if the customer stays vigilant throughout the scam by verifying new transactions and updating the bank balance.

6.5 Scam 2:

There are fraudulent sellers who post their phone numbers on business listing websites, and upon making a purchase, they request prepayment through a UPI transaction. In these situations, the money is deducted but no product is sent to the recipients. It increases the likelihood of your UPI account being hacked even more. Unauthorized application downloads may cause this kind of problem. Additionally, dishonest merchants may occasionally request that you download these programs in exchange for money. Via these apps, scammers can extract personal information, including UPI details. [b]

6.6 Scam 3:

Fraud rings gather money in a well-planned scheme by obtaining UPI data and keeping it in a different account. Similar to a money mule, this intermediary account handles payments from many sources. Citizens can protect themselves from this scam by safeguarding their UPI data.

6.7 Scam 4:

One popular UPI fraud that occurs when you click on phishing emails is malware. These

emails often offer their victims large sums of money or cash prices and include malicious links that can lead you to untrusted websites or download suspicious third-party software. Fraudsters may then duplicate your transaction information and utilize it improperly. Scanning emails for viruses and reporting suspicious emails can be helpful to avoid this. There have been instances where scammers offer amounts of money to their victims by falsely claiming that they have won cash prizes. They send a payment request for that amount and the victim types in their UPI pin in hopes of receiving that particular amount. The victim subsequently loses that amount from his account. It is good to note that people do not have to type in their UPI password to receive any amount.

6.8 Scam 5:

Certain perpetrators create fraudulent web pages that mimic legitimate UPI interfaces. Victims, often misled through phishing messages or emails, unknowingly enter their UPI credentials, PINs, or OTPs on these deceptive pages. The scammers then exploit this information to conduct unauthorized transactions. To avoid falling victim, users must exercise caution, verify the authenticity of payment pages, and refrain from sharing sensitive information on unfamiliar platforms.

6.9 Scam 6:

Store owners or merchants can be tricked by counterfeit UPI apps that resemble quite closely to famous UPI apps like Paytm or PhonePe which lets the scammer enter the total cost of items and the name of the outlet to mimic legitimate transactions. This allows the scammer to leave the shop with unpaid items leaving cashiers unaware of the fraudulent activity. Store owners or cashiers must remain vigilant and verify the authenticity of payment apps to prevent such a scam.

7. Preventive Measures for Users:

UPI is the easiest way to transfer funds, which makes the lives of millions of individuals a lot more convenient but more exposed to scams. Here are some tips listed below to keep you safe from fraudsters.

1. PIN Protection

UPI pin is the most important layer of defense which denies unauthorized access to your bank accounts. Regularly updating your device with the latest security patches, and using strong, unique passwords can help you keep safe from the vulnerabilities that can be exploited by the fraudsters. Another crucial aspect to be remembered is, never to share your UPI, PIN, and

OTP over the phone with people who claim to be government officials or bank employees. Remember the bank will never ask for your PIN or UPI. Hence, if someone is seeking your pin it's evident that it's a malicious entity.

2. Change pin regularly

It is recommended to change your PIN monthly or at the very least quarterly to safeguard yourself from potential threats. Routinely refreshing your PIN can be a good practice for individuals to keep their accounts safe and secure.

3. Utilize a secure network connection

Refrain from using public WiFi for making financial transactions, it may inadvertently aid hackers and give them a chance to access everything on your device. It is always advised to make use of secure networks when making financial transactions.

4. Employing two-factor authentication

Normalizing the use of two-factor authentication for UPI can sound like a hassle for the majority of individuals but it serves as an extra layer of security which drastically reduces the risk associated with our transactions.

5. Avoid clicking on any suspicious links received via SMS or email

Mails and SMS with enticing offers that are too good to be true are often encountered by almost every individual. Refuse to click on such links as they may direct you to phishing sites that replicate the appearance of a trusted organization or services which may result in the compromise of your security.

6. Refrain from responding to unsolicited payment requests

Exercise caution when confronted with sudden payment demands. Continue with the payment only if you are 100 percent sure that the individual on the receiving end is legitimate. As per the Financial Express, BHIM users are receiving payment requests from anonymous entities, and NPCI has cautioned users against accepting specific requests.

7. Monitor your financial transactions and bank account statements regularly. Remain vigilant for signs of suspicious activity. Banks must be quickly alerted if they detect any unusual activity.

8. Do not disable push notifications and transaction alerts on UPI apps.

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 14 Issue 02, February -2024,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

8. Technological Solutions

Technological solutions are imperative in preventing UPI scams as they focus on improving the overall security of UPI platforms which requires continuous innovation to ensure the integrity and trustworthiness of the UPI ecosystem. Let us take a look at some implemented solutions as well as some proposed solutions.

8.1 Government Initiatives:

In 2018, NPCI launched UPI 2.0 to introduce a wide range of features such as an overdraft facility, one-time mandate, invoicing, signed intent, and QR facilities under the umbrella of UPI. Signed intent and QR facility lets users verify the authenticity of merchants when scanning QR codes [8]. Even after the release of UPI 2.0, it still did not solve the weakness of UPI registrations where only the knowledge of a cell number and the ability to receive one SMS message from that number is required. Banks in India accept any cell number that the user registers with their accounts and there is not enough verification to know if the cell number registered actually belongs to the user which can be a concern [9].

In order to improve the security of UPI transactions, the Reserve Bank of India has suggested a four-hour cooling-off period for users initiating first payments to new receivers exceeding □2,000. This allows users to undo or alter transactions within the allotted duration. Currently, a user can transmit up to □5,000 in the first 24 hours after opening a new UPI account. With the National Electronic Funds Transfer (NEFT), □50,000 (wholly or partially) can be transmitted within a day once a beneficiary is activated. But under the new idea, each time a user pays more than □2,000 to a user they have never transacted with previously, a 4-hour time limit would be imposed. Four hours are given to the user to reverse or modify payments they made to a first-time user [10]. This can help prevent scams in a way if implemented carefully.

To build customer trust and satisfaction, the government can conduct standardized secure procedures by verifying and marketing UPI apps based on their safety, security features and data protection. This can decrease fraudulent activities such as scams where cybercriminals engage in the usage of malware or fake payment gateways. The government can compile and release a list of reliable and safe apps that people can download from their separate app stores by examining various apps, their technology, updates and other aspects. Putting in efforts to verify apps and protect user data, has the potential to have a positive effect and eventually contribute to a safe UPI ecosystem.

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 14 Issue 02, February -2024,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

8.2 Initiatives by various app stores:

App store verification of UPI apps is a necessity for ensuring customer safety and protection in the digital payment landscape. This establishes standardized safety and security measures that will help to build trust among users and reduce fraud. They can implement various strategies like filtering out suspicious payment apps or investigating them thoroughly. This process can provide ease for customers to choose a reliable UPI payment app to download.

8.3 User Awareness and Education:

User awareness is crucial for UPI apps to empower individuals against potential scams and security threats as well-informed users are better equipped to recognize common scam tactics and to adopt secure practices which let them stay vigilant against fraudulent activities. User awareness promotes a proactive approach which encourages individuals to verify information, report suspicious activities and maintain a cautious stance.

Governments play a vital role in spreading awareness about UPI scams by implementing multifaceted strategies. These include public campaigns through various media, collaboration with banks for information dissemination, educational materials, workshops, community outreach, integration with school curricula and leveraging official websites and apps. The government can ensure regular updates, collaborate with industry stakeholders, establish feedback mechanisms to foster a two-way communication channel and more. These efforts can lead citizens to have better knowledge about UPI scams and can promote secure digital practices.

UPI apps can prioritize user safety by providing comprehensive safety information such as best practices and tutorials. These resources can educate users on secure digital practices, including setting strong passwords, enabling multi-factor authentication and recognizing common scam tactics. These tutorials can guide users through the app's security features ensuring they understand how to protect themselves from potential threats. Updating educational content to address emerging threats and ensure users are equipped to navigate the evolving landscape of UPI security is vital. Approaches like these align with the broader industry trend of combining technology with user education to enhance overall cybersecurity awareness.

8.4 Integration of AI and Machine Learning:

Following the Google for India Event 2023, Google Pay Vice President Ambarish Kenghe claimed that scams of 12,000 crore rupees that could have taken place because of the unknowingness of UPI users have been prevented through Google’s fraud prevention

mechanism. Artificial intelligence and Machine learning were integrated to detect such scams. Integrating AI and ML into UPI fraud detection mechanisms enhances the ability to prevent scams effectively. These technologies analyze real-time transaction data, identifying patterns and anomalies associated with fraudulent activities which can be used to warn users. AI and ML continuously learn and adapt, enabling them to detect emerging threats and evolving scam tactics. By automating decision-making processes, these systems provide quick responses to potential risks, offering a proactive approach to UPI security. Behavioral analytics and dynamic modeling further contribute to the effectiveness of AI and ML in identifying deviations from normal user behavior.

These are several solutions that have either paved the way or hold the potential to establish an enhanced, secure and safe UPI ecosystem.

9. Conclusion

The Unified Payments Interface stands as a groundbreaking real-time payment system in India and its success has also attracted cybercriminals who seek to exploit vulnerabilities for financial gain.

Different types of scams have been reported, ranging from phishing attacks to QR code manipulations and the creation of fake UPI apps. The damage caused by UPI scams includes financial losses for individuals and businesses, erosion of trust in digital payment systems and potential disruptions to financial stability. Scammers often exploit the real-time nature of UPI transactions making it challenging to reverse unauthorized transfers promptly.

Preventive measures against UPI scams are paramount. Users are advised to adopt robust security practices. Governments and regulatory bodies play a vital role in implementing preventative measures. They establish and enforce security standards for UPI apps by conducting regular audits and collaborating with financial institutions to enhance the security infrastructure. User awareness is a linchpin in the battle against UPI scams. Awareness of potential risks and safe transaction practices should be spread through public awareness campaigns, workshops and other educational initiatives. In conclusion, while UPI has revolutionized digital payments, the prevalence of scams underscores the need for continuous efforts in user education and robust security practices. Stringent regulatory measures are crucial to evolve this ecosystem into a safe and secure one. It is the collective responsibility of users, government bodies, app companies and financial institutions to maintain the integrity and security of the UPI ecosystem.

International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 14 Issue 02, February -2024,
ISSN(O): 2249-3905, ISSN(P) : 2349-6525 | Impact Factor: 8.202| Thomson Reuters ID: L-5236-2015

References

[1] *About NPCI - Enabling digital payments in India | NPCI*. (n.d.). National Payments Corporation of India. https://www.npci.org.in/who-we-are/about-us

[2] *Unified Payments Interface (UPI) Product Statistics | NPCI*. (n.d.). National Payments Corporation of India. https://www.npci.org.in/what-we-do/upi/product-statistics

[3] Pti. (2024, January 20). Fraud cases in banking sector rises in first half of FY'24: RBI report. *The Economic Times*. https://economictimes.indiatimes.com/industry/banking/finance/banking/fraud-cases-in-banking-sector-rises-in-first-half-of-fy24-rbi-report/articleshow/106326609.cms

[4] Doffman, Z. (2019, August 10). Google warning: Tens of millions of Android phones come preloaded with dangerous malware. *Forbes*. https://www.forbes.com/sites/zakdoffman/2019/08/10/google-warning-tens-of-millions-of-android-phones-come-preloaded-with-dangerous-malware/?sh=52304f1bddb3

[5] *Reserve Bank of India - Notifications*. (n.d.). https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=12032&Mode=0

[6] Cio, E. (2017, March 31). Bug in UPI app costs Bank of Maharashtra Rs 25 cr in one of India's biggest financial frauds. *ETCIO.com*. https://cio.economictimes.indiatimes.com/news/digital-security/bug-in-upi-app-costs-bank-of-maharashtra-rs-25-cr-in-one-of-indias-biggest-financial-frauds/57930857

[7] *Cyber Security Final 03-10-2022*. (n.d.). https://www.ugc.gov.in/e-book/Cyber_Security/mobile/index.html

[8] Prasad, D. (2023, August 22). NPCI launches UPI 2.0: Here are top new features. *A Comprehensive Guide to Money Transfer, Recharges, Bill Payments and Other Digital Payments | Paytm Blog*. https://paytm.com/blog/payments/upi/npci-launches-upi-2/

[9] Kumar, R., Kishore, S., Lu, H., & Prakash, A. (2020). Security analysis of unified payments interface and payment apps in India. In *29th USENIX Security Symposium (USENIX Security 20)* (pp. 1499-1516).

[10] Barik, S., & Magazine, A. (2023, November 28). To curb fraud, 4-hour delay likely in first UPI transfer over Rs 2,000. *The Indian Express*. https://indianexpress.com/article/india/to-curb-fraud-4-hour-delay-likely-in-first-upi-transfer-over-rs-2000-9044890/

[11] Express News Service. (2024, February 28). 3 bank officials held in UPI scam case in Gurgaon. *The IndianExpress*. https://indianexpress.com/article/cities/delhi/gurgaon-cybercrime-case-bank-officials-arrested-9185238/

[12] *Mumbai woman foils UPI fraud bid after recognising 'Red flags'* (n.d.). NDTV.com. https://www.ndtv.com/india-news/bombay-woman-foils-upi-fraud-bid-after-recognising-red-flags-4809856

[13] Ani. (2023, December 19). AI voice fraud scam: Cyberthug dupes Lucknow man of Rs 45,000. *The Economic Times*. https://economictimes.indiatimes.com/tech/technology/ai-voice-fraud-scam-cyberthug-dupes-lucknow-man-of-rs-45000/articleshow/106109422.cms?from=mdr

[14] GfG. (2022, September 14). How does UPI work? GeeksforGeeks. https://www.geeksforgeeks.org/how-does-upi-work/

[15] Radhika Basavaraj Kakade- Prof. Nupur A. Veshne et al (2017), Unified Payment Interface (UPI) - A Way Towards Cashless Economy, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 11 | Nov -2017, Page no. 762 to 766.

[16] Dr. Kratika Neema-Dr. Arpit Neema et al (2018), UPI (Unified Payment Interface) –A new technique of Digital Payment: An Explorative study, International Journal of Current Research in Multidisciplinary (IJCRM), Vol. 3, No. 10, (October'18), Page no.1 to 10.