Herbert Wertheim College of Engineering
Department of Computer & Information Science & Engineering
UNIVERSITY of FLORIDA

Why UPI fails

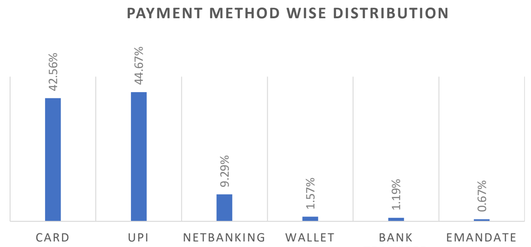
Abhiti Sachdeva, Yagya Malik

UF UNIVERSITY of FLORIDA

WORKING

Big Idea

Unified Payments Interface (UPI) is a system that allows a user to access multiple bank accounts with a single mobile application which merges seamless fund routing and merchant payments under one hood. This system can either be used through the participating bank's official mobile application or through third-party apps like Google Pay and PayTm (These are called payment service providers or PSPs).



(Data collected from RazorPay, an online-payment gateway used widely in India)

Working

PSPs – Allows customer to initiate/complete UPI transactions, authenticates payee.
VPA - A globally unique identifier assigned by the PSP (username@psp-handle)
NPCI – Acts as a switch to connect banks to PSPs, serves as a repository to keep track of VPAs
Banks – Responsible for debiting payee and crediting beneficiary

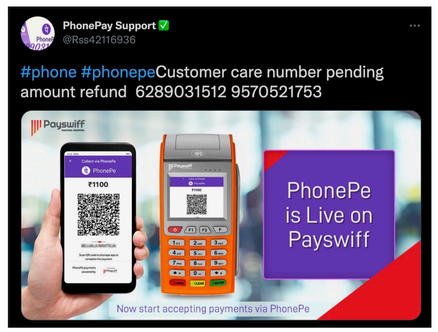
CHALLENGE

Request Money Fraud

An adversary, pretending to be a trusted party (e.g., representative from the user's bank), can gain access to a user's bank account details, or withdraw money from a user's bank account without knowing the user's bank account details such as their PIN, credit card details, or even their VPA by exploiting a feature known as Request money.
Collect Calls – This feature is unique to UPI wherein a user can send a payment request to another user in the form of a QR or a link with the help of their phone number for instant fund transfer.
The adversary can manipulate their VPA and profile picture to look like the real deal

Sample payment requests on PhonePe

Malicious numbers – Adversaries use smart techniques such as Social Media posts and carefully designed websites to spread these numbers.



METHODOLOGY

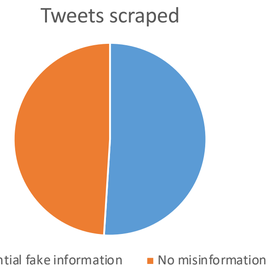
Approach

To investigate how this fake customer support information spreads on social networking sites, we began searching for fraudulent information on websites like Facebook and Twitter. We noticed that the most common terms in these posts were "get refund", "customer care no", "cashback offer", etc.

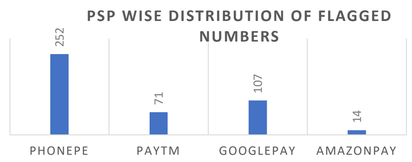
Experimental analysis

We used snscrape, which is a social networking service scraper in Python, to scrape tweets from Twitter querying them by the popular terms we observed before.

Out of the 10,000 tweets we scraped, 51% of them contained customer care numbers for PayTm, PhonePe, AmazonPay and GooglePay.



We designed an algorithm wherein we took all the contact numbers that were mentioned in the tweets and assigned them a score based on the number of times they were mentioned and the number of times the tweet containing that number was retweeted. We then generated a list of flagged numbers and distributed them by the PSP they were listed for.
The results were:
100% of the flagged numbers from our algorithm were fraudulent i.e., they were not who they claimed to be



SOLUTION

Advice by NPCI, PSPs and Banks

- Double-check the UPI ID before clicking on "send money"
- Find genuine support details in the Help/Support section of your PSP. Avoid untrusted numbers which may be listed on the Internet.
- Keep anti-virus and biometric recognition software installed.
- Never open emails or links from unknown source
- None of these are effective in stopping this attack.

Our solution

Every application that we worked with has a feature that warns users in case they are making a payment to someone that is not in their contacts. This does not seem to solve anything. Whereas our system can be used by PSPs and Banks alike to stay updated about fraud numbers and implement it as a feature in their application to warn the user if they are making a payment to one of the flagged numbers. As of February 2021, more than 300,000 cases of UPI frauds and scams have been reported. The information that the algorithm provides may be used by local police departments to track down organizations that run these scams on large scales.

Future Scope

Currently, our program analyses data only from Twitter. However, these fraudulent numbers can be found on Facebook, Google and many other websites. Since Facebook does not allow querying by terms in the posts, we could not test our system on it. Scope of our program can be further extended by modifying it to run dynamically to constantly update the list of flagged numbers as more tweets come in.

Takeaway - The request money fraud has become an immense security threat to the otherwise highly-secure system that is UPI. Our system can stop this attack from prevailing on social networking platforms and help banks and users stay safe from the scammers out there.