Beware of these 4 frauds while making payments via UPI amid lockdown

BY NAVNEET DUBEY, ET ONLINE | UPDATED: MAY 13, 2020, 02.17 PM IST

Post a Comment

Today, along with keeping oneself safe from the coronavirus, one has to be mindful of cybercriminals. These criminals are especially targeting users taking the digital route to conduct financial transactions.

Big Change:
The end of Five-Year Plans: All you need to know

One of the channels seeing a rise in frauds is the Unified Payment Interface (UPI), a digital payment platform that facilitates cashless, real-time transactions via mobile phones.

Several banks have issued advisories on their social media platforms warning customers of the same and have asked them to practice 'safe banking'.

It is important for all to note: @HDFC_Bank will never ask for your #OTP, #NetBanking/#MobileBanking password,… https://t.co/R1LdzrdlNa — HDFC Bank News (@HDFCBankNews) 1586437128000

Beware of the fake UPI IDs that are making the rounds in the guise of Prime Minister’s Citizen Assistance & Relief… https://t.co/8iNQW1rcWe — State Bank of India (@TheOfficialSBI) 1585574671000

Various types of frauds take place on the UPI platform. You should know that none of these are due to the issues with UPI itself but are modes

of deception.

How fraudsters can trap you

1. Phishing scams

Fraudsters can send you unauthorised payment links via SMS. These fake bank URLs will look almost identical to the original URL. If in a hurry you click on that link, it will direct you to the UPI payment app installed on your phone and will ask you to select any of the apps for auto-debit. Once, you give permission, the amount will get debited from the UPI app instantly.

Rajesh Mirjankar, MD & CEO, Infrasoft Technologies, a Mumbai-based fintech firm said, "Do not click on links in any SMS, especially those from unknown agencies. It could be an attempt to skim money from your account via UPI app. Also remember, the name is not everything on the Internet. For example, www.my.banker.com is not the same as www.mybanker.com. Make a note of the official website and official email ID of your banker, stockbroker, etc., directly from their representatives or official website."

Also, by clicking on the fake URL, it may infect your phone with a virus/malware designed to steal the financial information stored on the device.

Further, Pranjal Kamra, CEO, Finology, a Raipur-based Fintech firm, said, "You should never search for the customer care number on Google. If you have an issue with your transaction, register a complaint on the platform itself or get the number from the official website. With random Google searches you might end up calling a fake call centre," he said.

2. Remote screen mirroring tool

With work-from-home almost a mandate now, many people are downloading remote screen mirroring tools which can connect their phones or laptops through WIFI to larger displays like smart TVs.

Beware of fraudsters who pose as bank officials and scam people by gaining remote access to their mobile phone scre… https://t.co/AdgNZ4s1tQ — State Bank of India (@TheOfficialSBI) 1588782244000

However, not all digital payments app present on the on google play or apple app store are authentic, especially the unverified ones. Once you download an unverified app, it will take information from your phone and can have full control of the device.

Apart from this, fraudsters also conduct scams by posing as bank representatives who will ask you to download a third-party app for "verification purposes". Once downloaded, these apps will give them remote access to your phone.

3. Deceptive UPI handles

Just because a UPI social media page (Twitter, Facebook, etc.) has the word NPCI, BHIM or names similar to any bank or government organisation in it, does not make it authentic. Many tricksters create such handles to make you reveal your account details through a fake UPI app.

Kamra's advice is that one should not post their contact information on social media while trying to connect with a UPI brand. Generally, people put screenshots of message received on UPI handle. "The brand might not be able to reach your post, but a fraudster might notice it and contact you."

4. Scams using your OTP, UPI PIN

Bala Parthasarathy, Co-founder and CEO, MoneyTap, a Bengaluru-based fintech firm said, "A recent UPI fraud is hackers sending "request money" links to the customer. Once the customer clicks on the link and authorises the transaction thinking they'll receive money, the amount gets deducted from their account."

Another thing to be mindful is the OTP. When you make a transaction through your chosen UPI app, you are either required to enter the one-time password (OTP) or UPI PIN. For OTP authentication, your bank sends you an OTP through SMS on your mobile number registered with the bank. Once the OTP is verified, your transaction is processed.

Parthasarathy said, "One of the classic ways in which fraudsters try to scam people is by convincing them to share their UPI PIN and/or OTP over the phone. Once they have the details, they can authenticate UPI transactions and steal money from the customer's account."

Never share confidential details like UPI PIN, OTP, etc. with anyone on the phone. Also, banks never call you to ask these details.

What should you do in the case of digital fraud?

Sujay Vasudevan, Vice President, Cyber & Intelligence Solutions (C&I), Mastercard said that along with the application of best-in-class technology to prevent fraudulent transactions, the onus of keeping one's money safe lies with both - the banking and payment entities and the individuals. "Therefore, you need to be vigilant and stay guarded against fraudsters and avoid sharing confidential details like PIN, OTP etc. to keep your money safe," said Vasudevan.

Here are some things you can do to keep your money safe from fraudsters.

- Government agencies, banks and other financial institution never ask for financial information via SMS. In the case of a UPI fraud, report it to the bank or e-wallet firm and get the wallet blocked to prevent further losses. You can even report the incident to the police or the cyber-crime cell.
- You should download only those apps which are authentic and verified by Google Play Store or Apple Store.
- Never ignore the spam warning you get on your phone through the digital payments app. If a user has been reported earlier, a warning would show up while you are transacting with them. UPI apps like Google Pay, PhonePe, etc., alerts the user with a warning if they are receiving a request from an unknown account.

Click here to download ET Online's guide to everything personal finance in the times of Covid-19