CYBERSECURITY DIGEST

Bi-Weekly Update by the CISO Section of Meghalaya Rural Bank

Volume 1, Issue 6

Newsletter Date
01-12-2024

UPI Scam: The unprecedented surge

The rise of digitization in India has brought sweeping changes, with one of the most significant being the adoption of the Unified Payments Interface (UPI). Launched in 2015, UPI revolutionised banking by empowering popular apps like BHIM UPI, Google Pay, and PayZapp. Now, leaving home without cash is no longer a worry because your phone serves as your wallet.

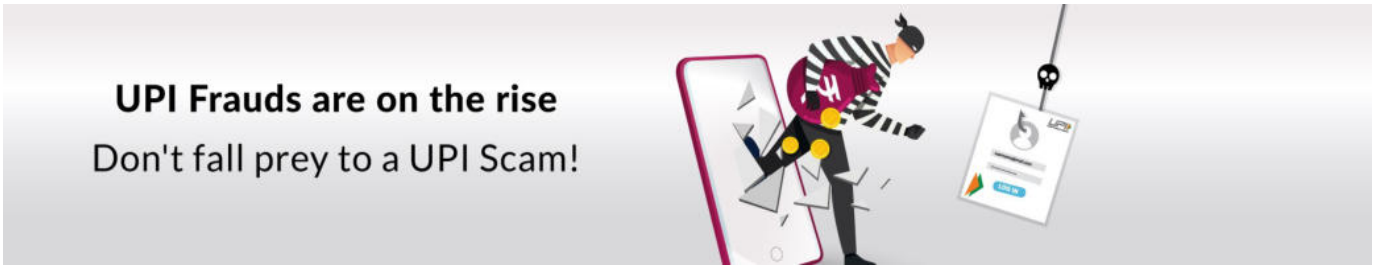
However, alongside its convenience, UPI has also brought challenges, notably in the form of scams like phishing scams, QR Code frauds, SIM swapping scams, fake payment apps and overcharging schemes. Cyber scams, already a prevalent threat, have amplified with UPI's popularity, leading to a surge in digital payment fraud in India. According to the RBI Annual Report, digital payment fraud reached a record 14.57 billion rupees ($175 million) in the fiscal year ending March 2024.

The main downside of UPI is that scammers who have your UPI ID can flood you with collect money or autopay requests. If you mistakenly approve these requests, you'll end up paying the fraudster, enabling them to use your money for their purchases.

The UPI scam operates on a simple principle-you are deceived into believing a false story or are caught off guard and approve an unknown UPI collect money or autopay request. You might wonder why you would approve such unfamiliar requests. The reason is that you may not be able to distinguish between a genuine request and a fraudulent one. It's important to note that the collect money or autopay request itself is valid, but the person initiating these requests is a fraudster.

UPI IDs are generally expressed as phone numbers followed by the UPI provider extension. This is exploited by scamsters. Phone numbers and details are soft targets since phone numbers are shared often and are quoted at multiple places - e-shopping, restaurants, malls, parking places and so on. Given that it's easy to crack UPI IDs, customers using the same for online and digital transactions need to be well aware of the risks. There have been a number of fraud cases in the past where customers have approved transactions thinking it's a receipt but have ended up transferring money from their account.

To safeguard against these threats, it's crucial to remain vigilant and exercise caution. Always verify the authenticity of communications and transactions, avoid clicking on suspicious links, secure your SIM card, and opt for secure UPI IDs for transactions. By staying informed and proactive, individuals can protect themselves from falling victim to these prevalent UPI scams and ensure safe digital transactions in an increasingly interconnected world.



How Do Hackers Execute UPI Fraud?

It's been observed that fraudsters follow a pattern whilst executing these elaborate plans. As a result, we've managed to weave a stepwise timeline of how these plans are generally performed. Let's take a look at how UPI fraud occurs:

- **STEP 1:** It all starts with a random call. Fraudsters usually call targets to get their attention, as opposed to texting. They commonly disguise themselves as a bank representative, calling for a seemingly harmless issue.
- **STEP 2:** To make the call sound legit, they proceed to ask verification questions like your date of birth, name, or mobile number.
- **STEP 3:** There is always a problem. Hackers use technical difficulties in the app or website to talk to you. They usually weave false stories that convince you to forfeit your personal information to resolve the issue.
- **STEP 4:** Once the fraudster has convinced you, they ask you to download an application on your phone. Some of these apps are AnyDesk and ScreenShare, which are available on the Google Play Store.
- **STEP 5:** While downloading AnyDesk or a similar application, it asks for privacy permission, like other regular apps. But don't be fooled; these apps can access everything on your phone.
- **STEP 6:** The fraudster will then ask you for a 9-digit OTP generated on your phone. As soon as you reveal the code, the hacker will also ask to grant permission from the phone.

STEP 7: When the app acquires all permissions required, the caller starts to take complete control of your phone without your knowledge. After gaining full access to your phone, the hacker steals passwords and begins transacting with your UPI account. Thus, you become one of the many victims of UPI fraud.

We identified other approaches, too. For example, fraudsters send an SMS and ask you to forward it to another number they provide. After the message is successfully sent, the fraudster can link your mobile number or account through UPI to their mobile.

Pagejacking

Page hijacking is a deceptive technique used by cyber attackers to manipulate web traffic. By creating a duplicate of a legitimate website, attackers aim to redirect users to a malicious site. This can be achieved by exploiting search engine algorithms, which may mistakenly prioritize the malicious site over the original.

Often referred to as 302 redirect hijacking or URL hijacking, this method involves using temporary redirects to trick search engines. The ultimate goal is to transfer the page authority and ranking signals from the legitimate site to the hijacker's site, thereby misleading users and search engines alike.

Traffic is the primary currency for securing and amassing revenue on the internet. This traffic and, ultimately, income is what pagejackers aim for, as they try to divert as much as possible from the original site.