यूको बैंक
UCO BANK

Protect Yourself from UPI Frauds

With the multi-fold rise of digital payments amid the pandemic, there has been a spike in UPI frauds aiming to trick innocent people of their hard-earned money. However, by staying cautious and vigilant, one can ensure that his money stays safe and he doesn't become a victim of UPI fraud.

Stay Alert... Stay Safe

Don't share financial details with anyone

- Keep your Debit / Credit Card PIN, CVV number & OTP secure.
- Do not use the same PIN for everything. If your ATM pin is the same as your UPI pin, you just leave yourself open to more chances of fraud.

Check the UPI ID

- Double check the UPI ID / beneficiary details and ensure it is the correct one before clicking the 'Send Money' button .

Don't enter UPI PIN while receiving money

- There are several incidents of scams where users have been tricked into entering their UPI PIN in response to a 'send money' request purporting as 'receive money' request from a fraudster.
- This usually happens when the user is looking to sell something and they are contacted by a fraudster who convinces them that they can 'receive' the money by entering their UPI PIN.
- Be vigilant! Remember that you do need not enter your UPI PIN to receive money. UPI PIN is required for sending money only.

Be wary of scam KYC calls

- Fraudulent phone calls appearing to be from Banks/Financial Institutions are doing rounds.

यूको बैंक
UCO BANK

Contd... Protect Yourself from UPI Frauds

- These callers convince users about the need to update their account's KYC details.
- They even warns the user of dire consequences such as losing access to their account if not complied and then asks to provide UPI PIN and other sensitive personal / financial data.
- Do not provide confidential financial data such as your UPI PIN on such a call.
- Always remember that Banks will never ask you for sensitive personal / financial information such as UPI PIN, net banking password or ATM Card number, OTP etc via phone calls / email or SMS.
- If you have received any such calls, report immediately to the nearest Cyber Crime Police Station & National Cyber Crime reporting Portal (www.cybercrime.gov.in).

Practice safe Banking

- Always open banking or other financial services websites directly by typing the URL in the browser. Do not attempt to access them by clicking on suspicious link received via mail/message.
- Pay attention to the URL. Remember, www.my.bank.com & www.mybank.com are not the same.
- Think twice before entering personal / financial details on the pages opened from links in unknown messages.

Beware of Remote Screen Mirroring apps

- Do not download / install unknown apps if prompted by random caller, posing as Bank executive, in context of redeeming reward points or settlement of transaction disputes.
- Be cautious before granting permissions to apps while installing them.
- Do not fall prey to traps of gift vouchers, scratch cards, lucky bonanza etc.

Ensure your devices are protected

- Keep OS and applications updated and antivirus installed in all devices to protect you from threats arising out of malicious software.

CISO, UCO Bank