CYBER SECURITY HANDBOOK

V FOR VIGIL AUNTY

An initiative by

HDFC BANK

Find her on

TABLE OF CONTENTS

01

Introduction

In today's digital age, banking is faster and more convenient than ever, but it also comes with new risks. Cybercriminals are constantly evolving their tactics to exploit technology and human behavior, targeting individuals and institutions alike.

This handbook is designed to help you recognize common fraud techniques, understand how scammers manipulate emotions, and learn simple yet effective steps to stay secure online. Whether you're managing personal finances or handling sensitive banking operations, this guide will empower you to protect yourself and your data in the digital world.

Remember, awareness is you best defense against cybercrime. Stay informed, stay vigilant, and stay safe!

In case you have been a victim of a fraud, report it on *https://www.cybercrime.gov.in/* or call *1930.*

02

Psychological Manipulation in Cybercrime

- How Scammers Exploit Human Emotions

How Scammers Exploit Human Emotions:

Cybercriminals often rely on psychological manipulation to deceive individuals and gain unauthorized access to sensitive banking information. Understanding how scammers exploit basic human emotions can help protect both employees and customers from falling victim to fraud.

Below are key emotional triggers commonly used in cyber scams:

Greed:
Fraudsters entice victims by appealing to their desire for financial gain. Phrases like "You've won a cashback or lottery" are designed to trigger excitement and distract from logical evaluation. Victims may unknowingly click on malicious links or provide personal data under the illusion of receiving a reward.

Threat/Fear:
Scammers instill fear to provoke quick reactions without rational thinking. A common tactic is sending alarming messages like, "You are under Digital Arrest." This fear of financial loss or account suspension compels the target to take immediate action, often ending in them sharing confidential information.

Help:
Scammers often impersonate trusted individuals or institutions such as bank officials, government representatives, family or friends using tactics like AI- generated voices or fake social engineering credentials that look authentic. This manipulation creates a false sense of urgency with messages like, "Respond immediately or lose benefits" intended to force quick decisions without verifying their authenticity.

03

Understanding Cybercrime

- Common Types of Cyber Frauds
- Modus Operandi of Fraudsters

Common Types of Cyber Frauds

Phishing
Deceptive emails or websites trick users into revealing sensitive banking information.

Vishing
Fraudsters impersonate bank officials over phone calls to extract confidential data.

Smishing
Fake SMS messages lure victims into clicking malicious links or sharing personal details.

ATM/Card Skimming
Card data is cloned using hidden devices at ATMs or payment terminals.

SIM Swap Fraud
Scammers hijack mobile numbers to intercept OTPs and access bank accounts.

QR Code Scam
Malicious QR codes redirect users to fraudulent payment or phishing sites.

Fake Banking Apps
Lookalike apps steal login credentials and financial data from users.

Remote Access Scam
Victims install apps that give fraudsters control over their devices.

Fake Cashback/Reward Scams
Fraudsters offer fake rewards to obtain card details and OTPs.

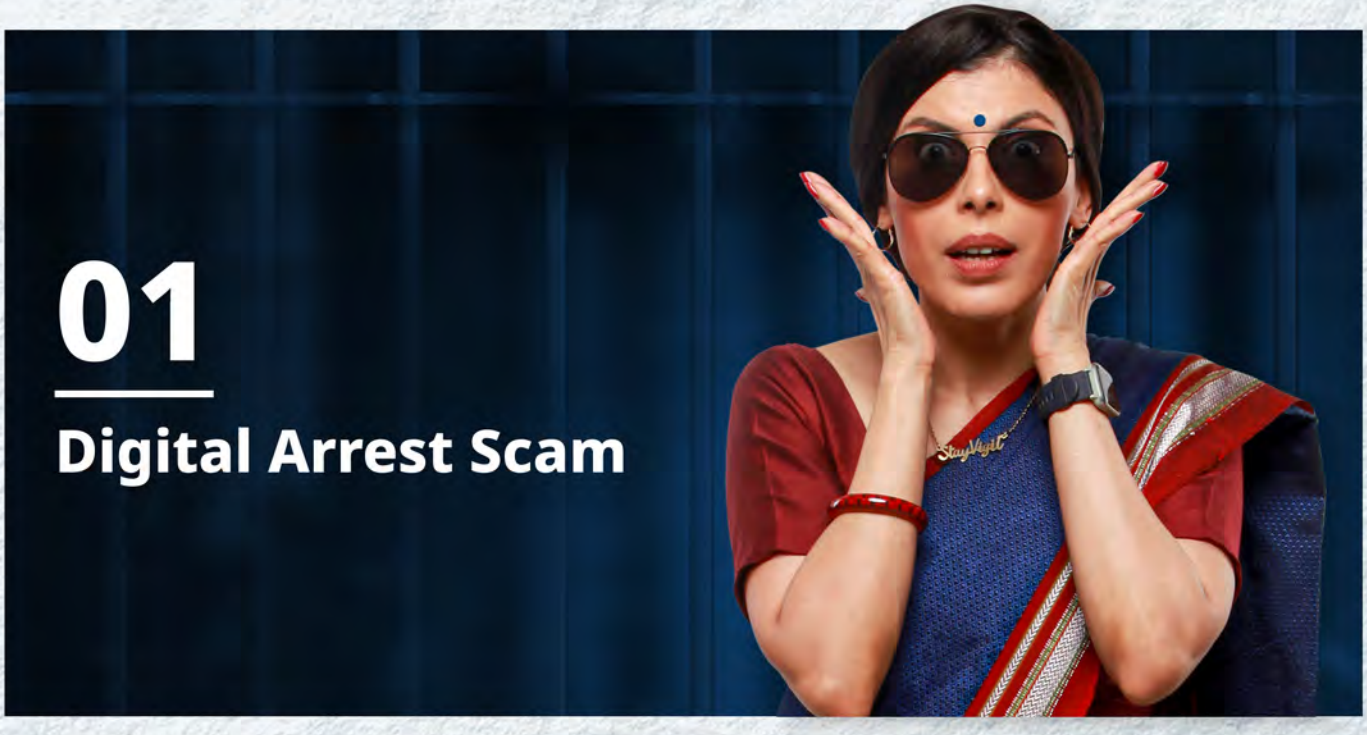
Social Media Impersonation
Scammers pose as bank staff on social platforms to solicit information.

Fake UPI Handles
Fraudulent UPI IDs divert payments during online transactions.

Malware/Ransomware Attacks
Malicious software locks systems or steals data for ransom.

Modus Operandi of Fraudsters

Cybercriminals employ sophisticated tactics to deceive individuals and gain unauthorized access to financial information. They often use fake identities, cloned websites, and psychological pressure to manipulate victims. Below is a breakdown of prevalent scams, how they operate, and how to stay protected:



Fraudsters impersonate officials from law enforcement agencies such as the police, CBI, Narcotics Bureau, or regulatory bodies like RBI. They falsely accuse the victims of serious crimes such as money laundering, tax evasion, or illegal parcel involvement and claim that an arrest warrant has been issued. To intensify fear and control, they threaten harm to family and loved ones, instruct victims not to leave their location, force them to stay on video calls under the guise of legal procedures, and demand immediate payment or sensitive information to avoid arrest.

Safety Tips:

- Law enforcement agencies never demand money or personal data or interrogate over phone or video calls.
- There is no such thing as “Digital Arrest”.
- When in doubt, consult your Relationship Manager or Branch before taking any action.

02

Investment Scam

Fraudsters lure victims through social media platforms, fake websites, or mobile apps, promoting high-return investment schemes that appear low-risk and highly profitable. To build credibility, they often share fabricated testimonials and success stories and may even make small initial payouts to gain the victim's trust. Victims are then added to WhatsApp, Telegram, or other social media groups where peer pressure and urgency are used to persuade them to invest larger amounts. Eventually, the scammers disappear with the funds, leaving victims with no recourse.

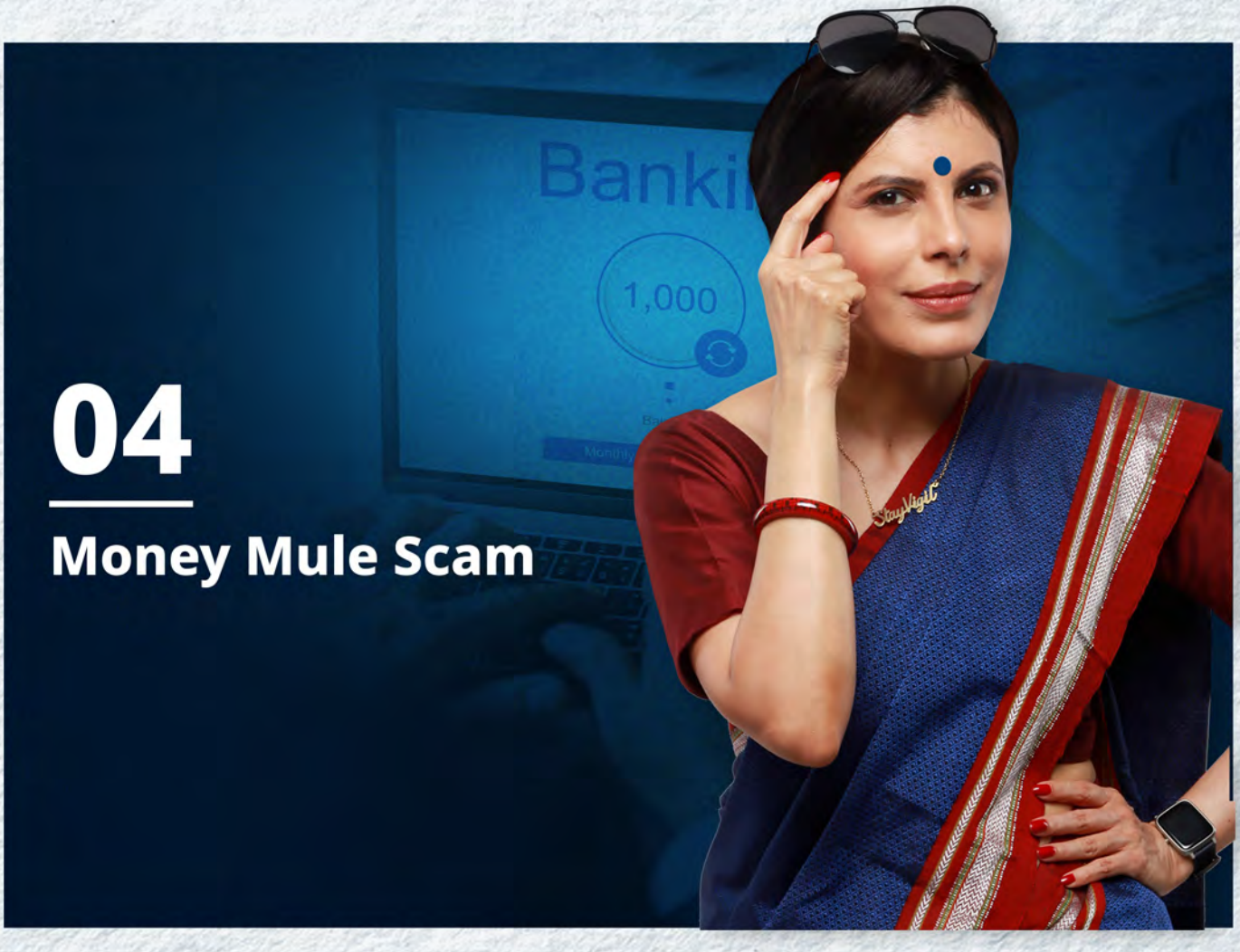
Safety Tips:

- Always verify investment platforms with SEBI or other official financial authorities.
- Be cautious of schemes promising unrealistic returns or guaranteed profits. Avoid transferring money based on social media promotions or unsolicited investment advice.
- Do not trust testimonials or group messages without independent verification. Exit and report suspicious WhatsApp/Telegram groups immediately.

Fraudsters trick victims into downloading malicious mobile applications (APK files) disguised as genuine links from trusted sources such as e-challan portals, income tax departments, police, or banks. Once installed, these fake apps grant remote access of the victim's phone to the fraudster, allowing them to view the screen, capture OTPs, read messages, and access sensitive banking information. The fraudsters then misuse this access to transfer money, steal personal data, and commit further cybercrimes like identity theft.

Safety Tips:

- Never download apps or click on links shared through messages, emails, or social media.
- Install apps only from official platforms like Google Play Store or Apple App Store.
- Verify the sender's identity before acting on any message.



04

Money Mule Scam

Scammers may deceive individuals into knowingly or unknowingly assisting in laundering illegal funds. This is done by convincing them to receive and transfer money through their personal bank accounts or offering payment in exchange for renting out their bank account. Participating in such schemes even unknowingly can support criminal activities and lead to serious legal consequences.

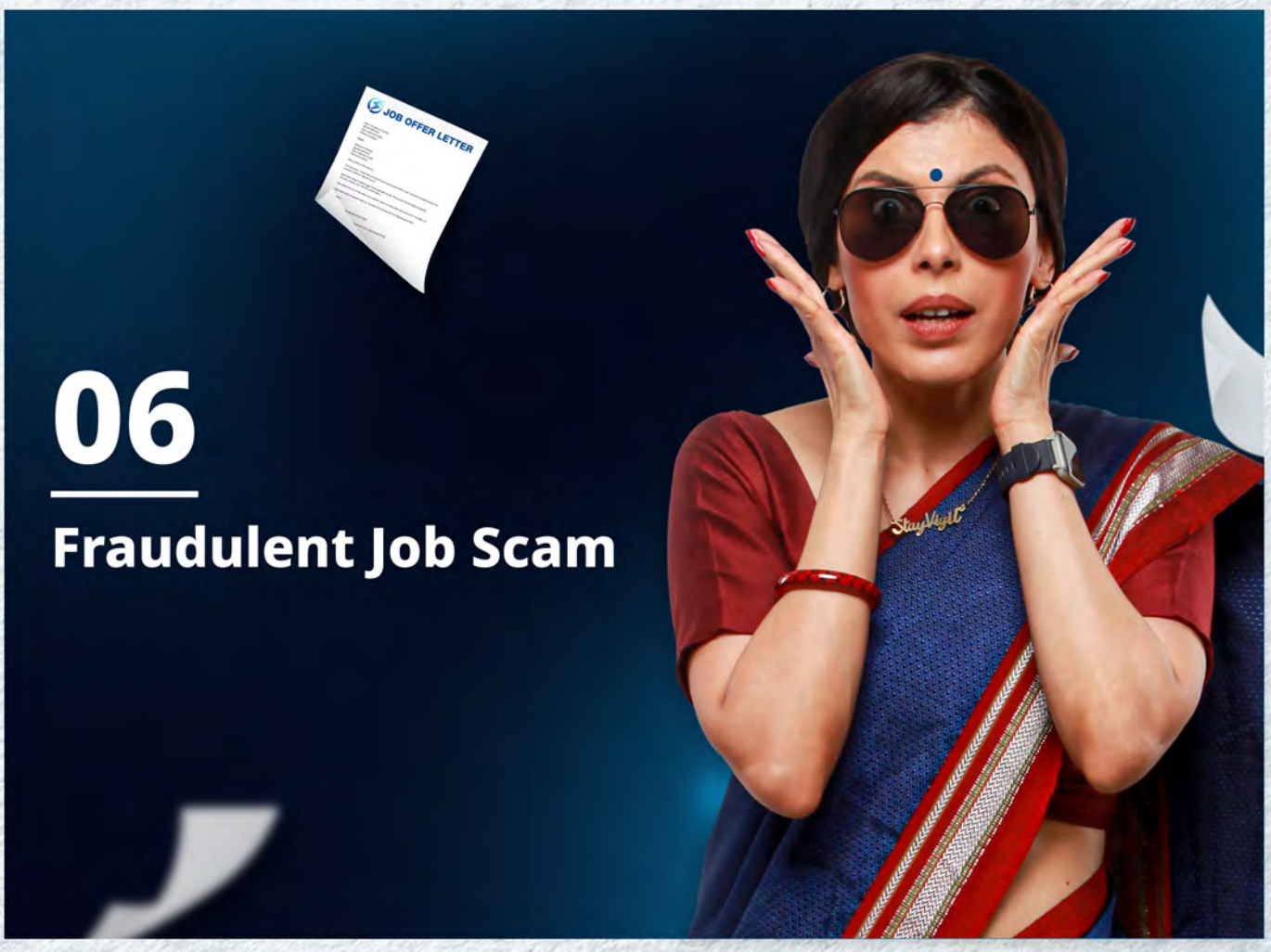
Safety Tips:

- Never share your bank account with unknown individuals or third parties.
- Do not get carried away by attractive offers/commissions or consent to receive unauthorized money.
- Be cautious of job offers that promise “easy money” with minimal effort or vague responsibilities.

Scammers pretend to be from courier or delivery services. They claim the victim has a package waiting and asks them to pay fake delivery charges, customs fees, or share personal information like OTPs, card numbers, or PINs. Their goal is to steal the victim's money/sensitive data.

Safety Tips:

- Check the courier's official website to track packages or confirm charges.
- Don't share personal or payment details without verifying the caller.
- Be cautious of unexpected calls or messages asking for customs duty or delivery fees.



06

Fraudulent Job Scam

Scammers trick job seekers with fake job offers. They ask for money for registration, training, or placement, and may also collect personal details pretending it's part of the hiring process.

Safety Tips:

- Real companies never ask for payment to give you a job.
- Verify the company and recruiter through the official website.
- Be careful of job offers that seem too good to be true - if there's no interview, it's likely a scam.

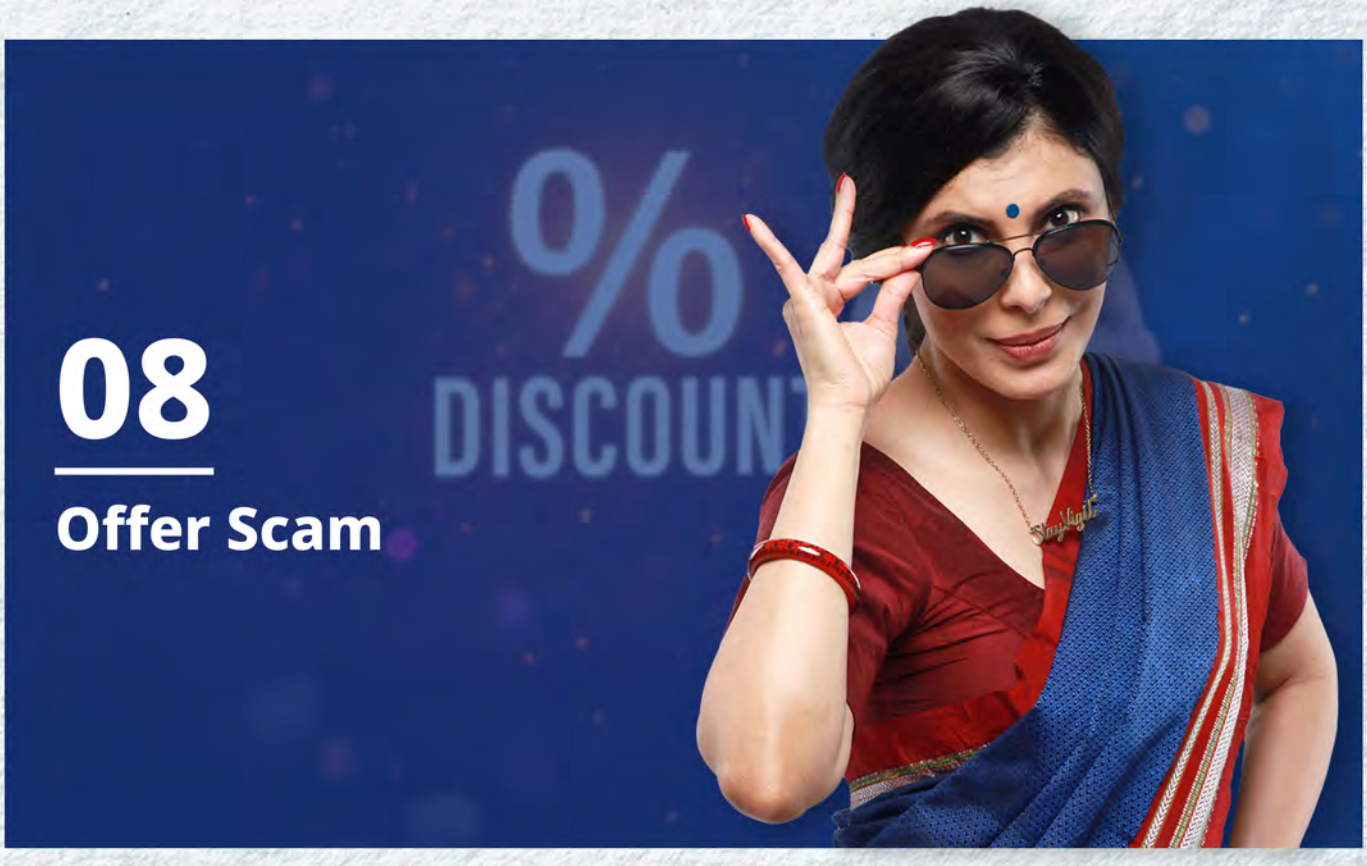
07

Deepfake Scam

Scammers use advanced technology to create fake videos, voice recordings, or images that look and sound real. These deepfakes may impersonate trusted people like company leaders, celebrities, or family members to trick victims into sending money or sharing sensitive information.

Safety Tips:

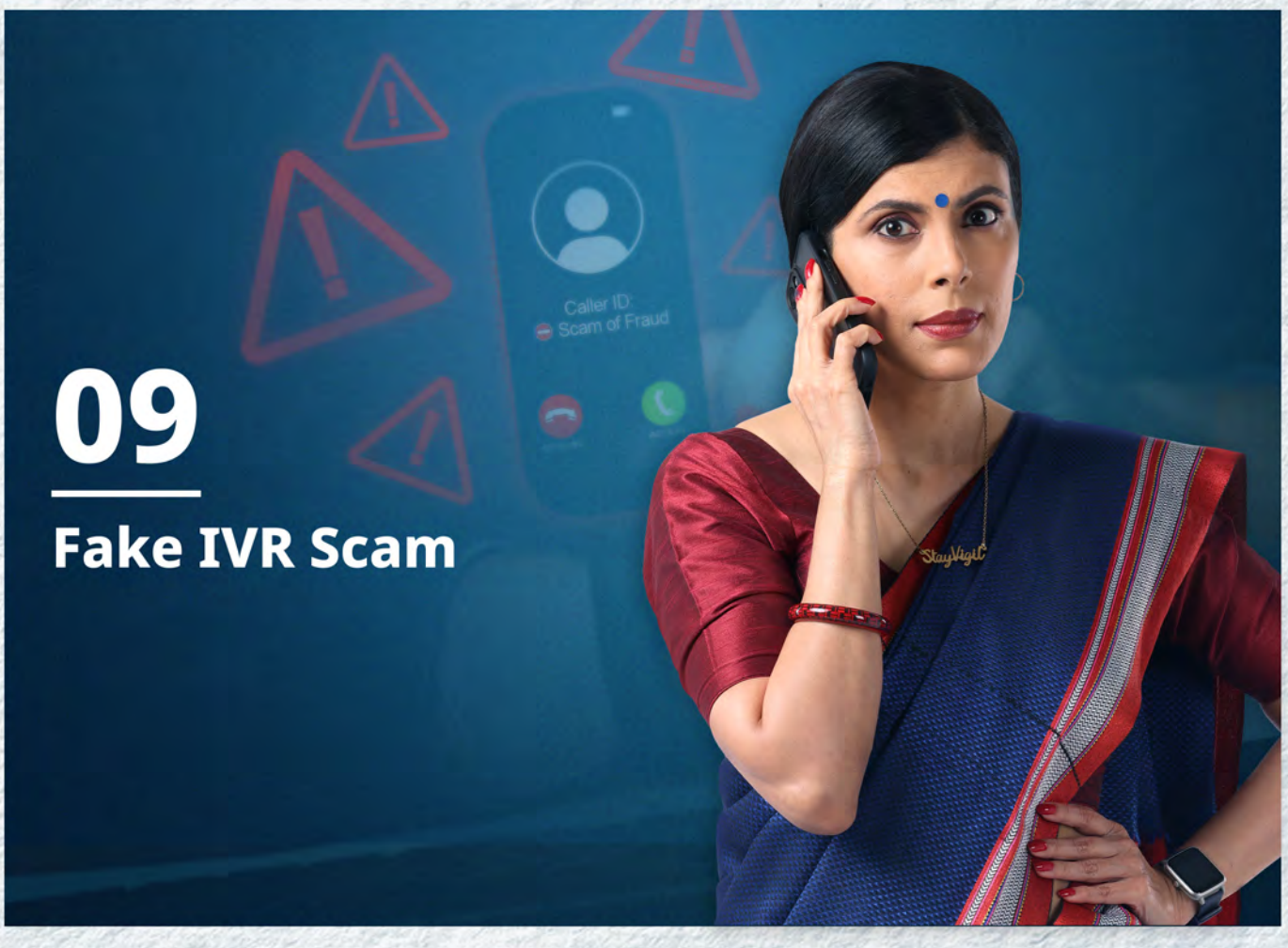
- Verify any unusual requests, especially if they involve money or personal information, even if they seem to come from someone you know.
- Don't trust videos or voice messages blindly; check with the person directly through a known contact method.
- Be cautious of emotional or urgent messages asking for quick action.



Fraudsters often lure victims with fake credit or debit card offers, reward redemption schemes, cashback promotions, card activation requests, or limit enhancement claims. These tactics are designed to trick individuals into sharing sensitive information such as card details and OTPs or clicking on malicious links.

Safety Tips:

- Never share your OTPs, card PINs, or any confidential banking information with anyone.
- Always use your bank's official app or website to access your account or avail offers. Alternatively, visit your nearest bank branch.
- Use only secure and trusted payment platforms for transactions.
- If you suspect fraud, immediately block your card and change your net banking password.
- Update your passwords regularly to enhance account security.



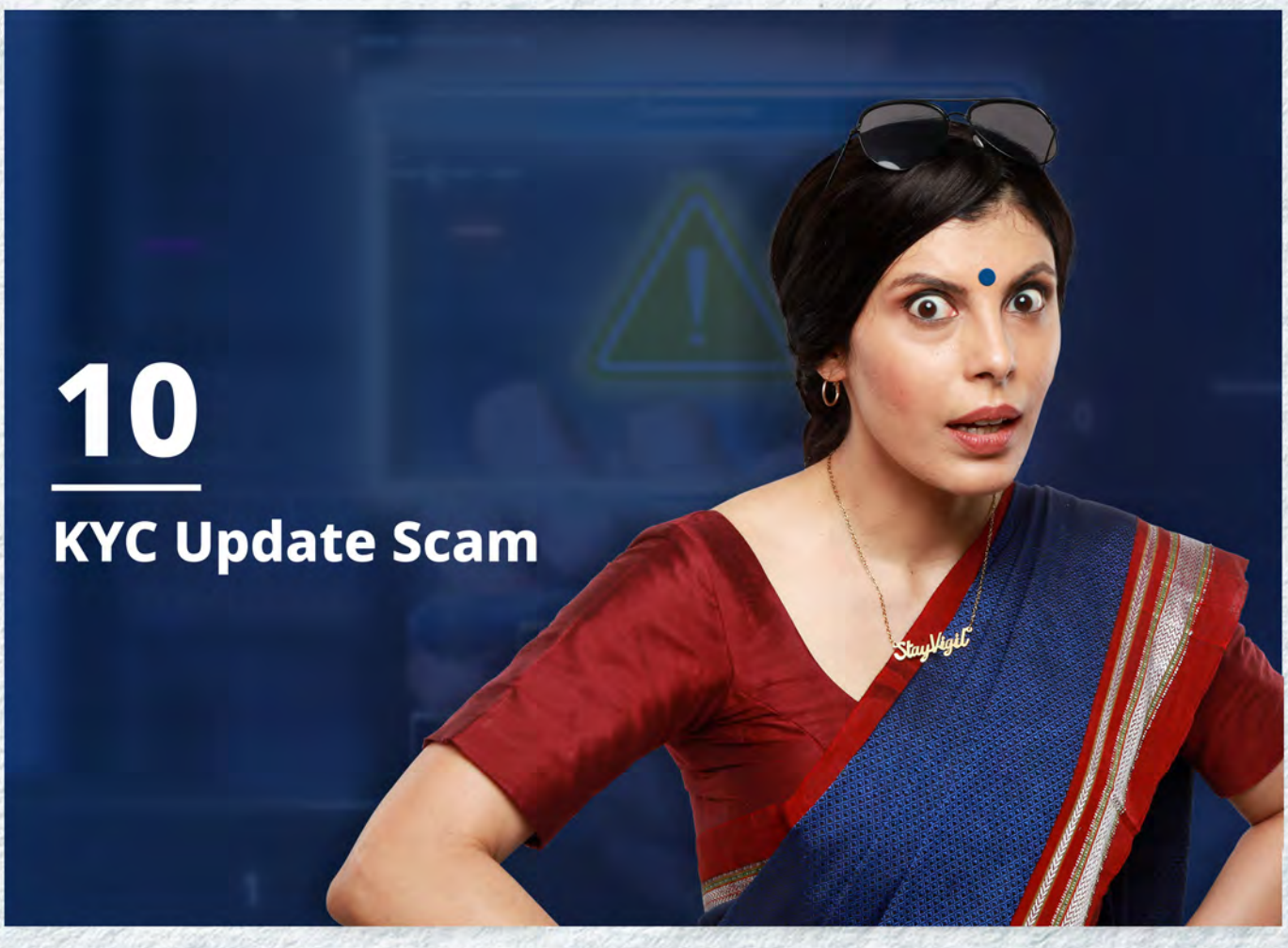
09

Fake IVR Scam

Scammers create fake automated phone systems (IVRs) that sound like banks, telecom companies, or government offices. They trick people into sharing sensitive details like OTPs, card numbers, or login credentials by pretending to help with verification, avail offers or solve problems.

Safety Tips:

- Always check helpline numbers on the official website before calling.
- Never share personal or financial details over calls you didn't expect.
- Don't press any buttons or follow instructions on suspicious or unknown calls.



Fraudsters pretend to be from a victim's bank or financial company and claim their KYC (Know Your Customer) details need urgent updating. They may call, message, or email the victim, warning that their account will be blocked if they don't act quickly.

Safety Tips:

- Don't click on unknown links in messages or emails.
- Visit your bank's branch or official website to update KYC.
- Never install apps suggested by strangers; they may give scammers access to your phone.

11

Utility Scam (Electricity/Gas)

Scammers pretend to be from electricity or gas companies. They claim there's a problem with the victim's bill or connection and threaten to disconnect their service unless they pay immediately. They use fear and urgency to trick the victim into acting without checking.

Safety Tips:

- Call the official helpline of your utility provider to confirm any issue.
- Don't download apps sent by unknown callers for payment/reconnection.
- Stay calm. Don't panic or rush into making payments.

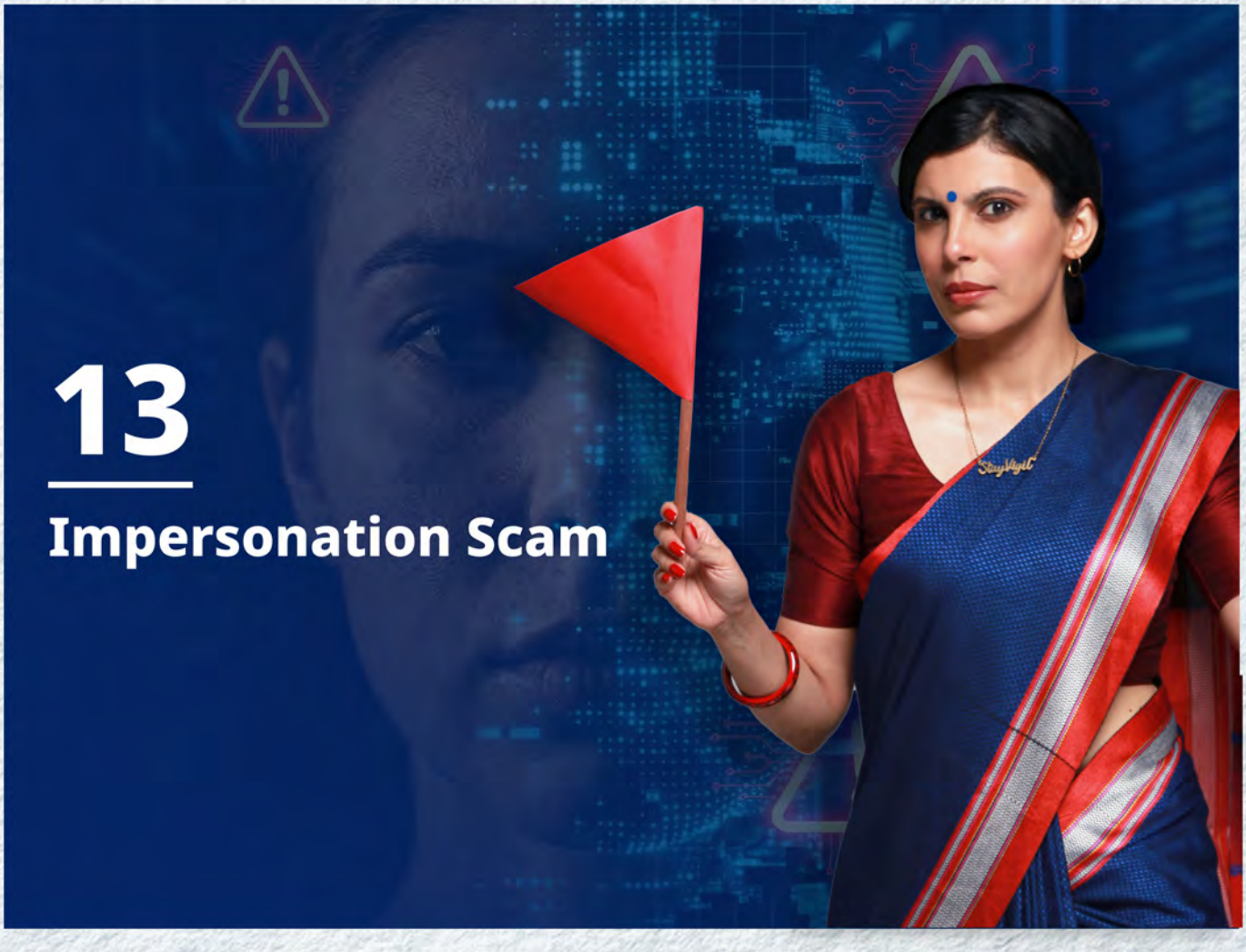
12

E-challan Scam

Scammers send fake messages or emails claiming the victim has unpaid traffic fines (e-challans). These messages often contain links or ask for immediate payment. Their goal is to trick them into sharing personal or financial details.

Safety Tips:

- Verify e-challans only on the official RTO website (like Parivahan or your state transport portal).
- Don't click on suspicious links/make payments through unknown sources.
- Be cautious of urgent messages demanding quick action or threatening penalties.



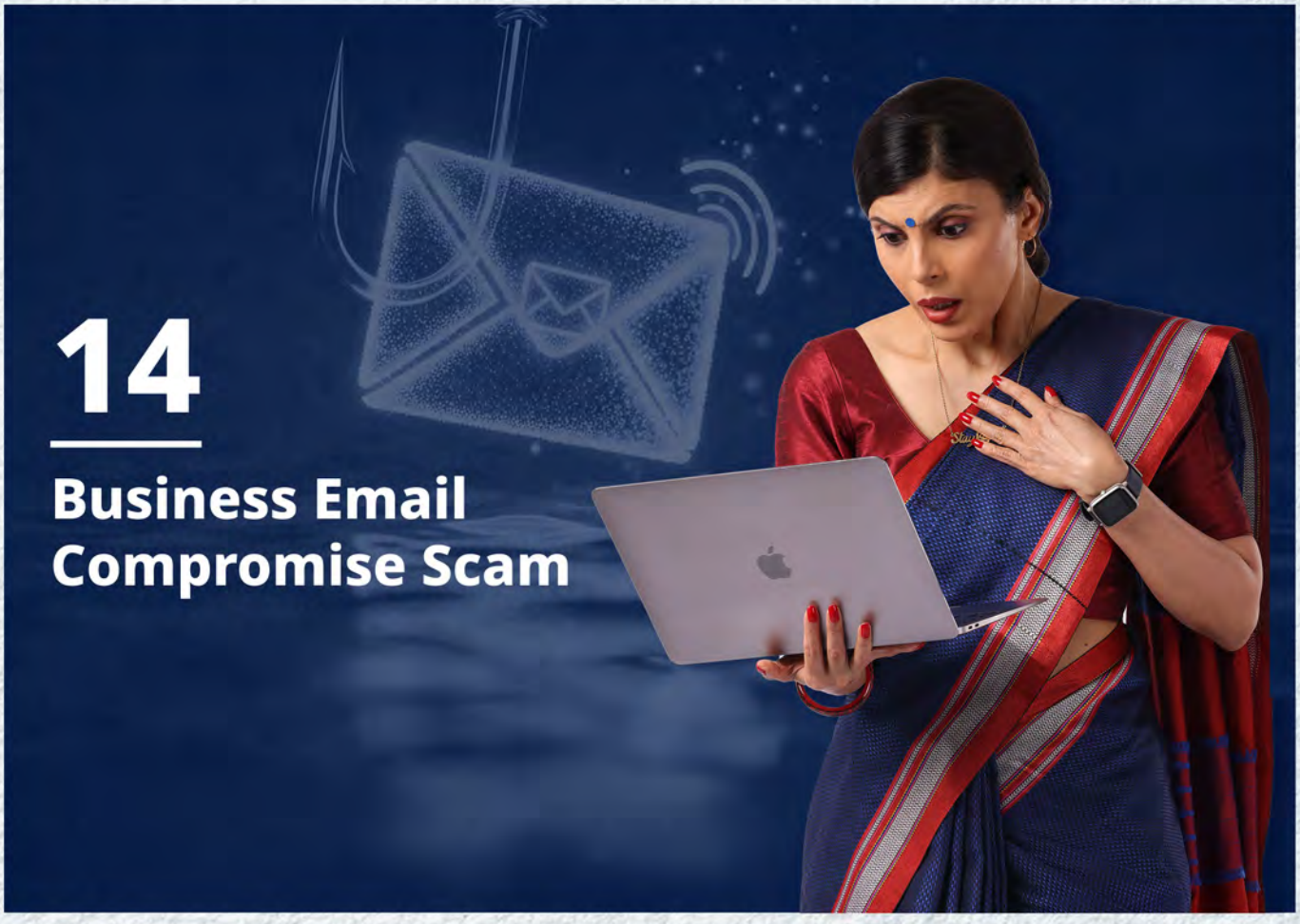
13

Impersonation Scam

Fraudsters pretend to be someone you know - like a friend, family member, or colleague - to trick you into trusting them. They reach out through calls, messages, emails, or social media platforms, often faking urgency to extract money or personal information.

Safety Tips:

- Always verify the request by calling back on a known number.
- Avoid sending money without confirmation.
- Be skeptical of urgent requests via messages.



14

Business Email Compromise Scam

Business Email Compromise is a fraud where scammers pretend to be your senior manager, vendor, or overseas business partner by using fake or hacked email IDs. They closely watch email conversations and, at the right time, send emails asking for urgent payments or changes in bank account details. These emails look genuine and create pressure to act quickly, which can lead to money being transferred to fraudsters instead of the real recipient.

Safety Tips:

- Always verify payment or bank detail change requests by calling the person or vendor on a trusted phone number before making any transfer
- Check email details carefully for small spelling errors, unusual sender addresses, or urgent language asking for secrecy or quick action.
- Strengthen email security and processes by enabling Multi-Factor Authentication (MFA), keeping vendor details updated, and following internal approval checks for all payments.

04

Safety and Security Guidelines

- General Cyber Safety Tips
- Mobile Device Security
- Secure Net Banking Practices
- Secure Online Shopping & Internet Browsing Tips

General Safety Tips:

1. Never share confidential banking details such as your Customer ID, Password, Card Number, CVV, Expiry Date, OTP, or PIN with anyone, not even with someone claiming to be a bank official or a law enforcement officer.

2. Avoid responding to unknown numbers, links, or messages. Fraudsters often send fake links or use look-alike numbers to trick you into sharing personal or financial details.

3. Do not download or install third-party apps from unknown sources or links shared over call/SMS/WhatsApp. These can give fraudsters remote access to your device.

4. Never share your screen with anyone or allow remote access through apps. Regularly review your call, SMS, and app permissions.

5. Stay alert against digital arrest scams. No government or law enforcement agency conducts arrests over video calls or asks for payments for investigation or bail.

6. Be cautious of investment scams. Do not transfer funds or invest based on promises of high or quick returns. Always verify through official bank or regulatory sources.

7. Beware of APK scams. Fraudsters may send links to download apps under the guise of offers, refunds, or payment confirmations. Such apps steal your data and enable unauthorized access.

8. Always verify beneficiary details before making fund transfers. Confirm with the receiver through a known and trusted source.

9. Avoid making transactions under pressure or emotional influence. Fraudsters often create urgency or fear to force quick action.

10. Check and verify URLs carefully. Fraudsters may use fake websites resembling genuine ones to collect your information.

11. Keep your mobile device, operating system, and antivirus updated for better protection.

12. Enable real-time transaction alerts through SMS, email, or the HDFC Bank Mobile App to monitor account activity.

13. Review your account statements regularly for any unauthorized transactions and report discrepancies immediately.

14. Do not believe calls claiming your account/card will be blocked unless you act immediately. Such claims are fraudulent.

15. Cross-verify communication from the bank, RBI, or any financial authority through their official website or contact number.

16. Report suspicious communication or numbers on the Chakshu Portal (*https://sancharsaathi.gov.in/*) or Sanchar Saathi App.

17. If you suspect fraud, act immediately:

    - Contact HDFC Bank Customer Care or visit your nearest branch.
    - Report the fraud on the National Cybercrime Portal *https://www.cybercrime.gov.in/*
    - Call the Cyber Helpline *1930* for immediate assistance.

18. HDFC Bank will never call you from its helpline numbers. If you receive a call from a number resembling our helpline, do not share any personal banking information.

19. Always verify before calling, visit the official HDFC Bank website to confirm the correct helpline number. You can also visit your nearest HDFC Bank branch for support.

Mobile Device Security:

Do's	Don'ts
• Lock your phone and banking apps.	• Don't store passwords in text format.
• Install apps only from official stores.	• Don't share your screen with anyone asking for sensitive details like PINs, CVVs or OTPs while making an online transaction.
• Report loss of phone immediately to the bank.	• Don't delete potential evidence.

Secure Net Banking Practices:

Do's	Don'ts
• Use strong, unique passwords.	• Don't use public Wi-Fi for banking.
• Log out after every session.	• Don't click on banking links in unsolicited emails or SMS.
• Monitor account activity regularly.	• Don't share login credentials.

Secure Online Shopping & Internet Browsing Tips:

Do's	Don'ts
• Shop only on secure and reputed websites (look for "https" and a padlock symbol)	• Don't shop using public Wi-Fi or shared computers.
• Use credit/debit cards with OTP verification for payments.	• Don't save card details on shopping websites.
• Log out after every transaction and keep transaction receipts.	• Don't click on suspicious ads or pop-ups.
• Keep browser and antivirus software updated.	• Don't download software from untrustworthy sites, including torrent sites.

05

Incident Response

- How to report Cyber Fraud
- Do’s and Don’ts After a Cyber Incident

Please Remember: Adopt the "LBW Rule" to Combat Frauds

To ensure timely action and minimize loss, HDFC Bank advises customers to adopt the LBW Rule:

L – Law Enforcement:
Victims should file a complaint on https://cybercrime.gov.in/ or call 1930 immediately.

B – Bank:
Contact your bank immediately if you notice any Credit, Debit, Net Banking, or UPI transactions not initiated by you.

W – Wipe:
Completely wipe your devices, change passwords, and ensure your device is clean and secure to prevent further misuse.

How to Report Cyber Fraud

Prompt reporting of cyber frauds can prevent financial losses and help authorities act swiftly. Follow the steps below in case of any suspicious or fraudulent activity.

If you are a victim of fraud,

💳 Immediately block your Debit/Credit Card using HDFC Bank Net Banking or Mobile Banking

📞 Call on Bank helpline 1800 1600 / 1800 2600 (accessible across India) to report the fraud.

⚠️ Report any type of cybercrime 24x7 at *https://cybercrime.gov.in/*

💰 For financial fraud, report immediately on the cybercrime helpline: 1930.

If you receive fake communication from:

- 🏦 Banks or payment apps
- ⚡ Electricity/Gas companies
- 👮 Government officials or fake relatives

Report it at the earliest at
https://sancharsaathi.gov.in/sfc/Home/sfc-complaint.jsp
or via the Sanchar Saathi mobile application.

Unsure about a message sender?

Check here: *https://smsheader.trai.gov.in*

Or send an SMS on 1909:
DETAILS <SPACE> OF <SPACE> CLI/HEADER

- 📱 Know the number of connections issued in your name by logging in using your mobile number.
- 🔢 Enter your mobile number, captcha & OTP. You can also report unnecessary or unauthorized mobile connections here
- 🔗 *https://tafcop.sancharsaathi.gov.in/telecomUser/*
  or via the Sanchar Saathi mobile application.

Lost your phone?

Block it to prevent misuse. Keep these ready:

- IMEI number
- Mobile number
- ID proof
- FIR copy

🚫 Block it here:
https://ceir.sancharsaathi.gov.in/Request/CeirRequestStatus.jsp
or via the Sanchar Saathi mobile application.

To report UCC or spam received through Voice Call or SMS which is not as per your consent or registered preference.

⚠️ File a complaint within 3 days at
https://sancharsaathi.gov.in/sfc/Home/ucc-complaint.jsp
or via the Sanchar Saathi mobile application.

Do's and Don'ts After a Cyber Incident:

Do's	Don'ts
• Immediately inform your bank and block your card/account.	• Don't delay reporting the incident.
• Collect evidence: screenshots, messages, URLs.	• Don't engage further with the fraudster.
• Report on government portals.	• Don't delete potential evidence.

06

Leadership Message

- Message from the Hon'ble Prime Minister Shri Narendra Modi Ji

Message from the Hon'ble Prime Minister Shri Narendra Modi Ji

Mann ki Baat

In an episode of Mann Ki Baat, Honorable Prime Minister, Shri Narendra Modi Ji awakened society to the menace of defrauding people by threatening them with a 'Digital Arrest'.

In a digital arrest fraud, fraudsters make calls impersonating officials from the police, CBI, Narcotics Bureau, or the RBI, acting as "fake officers" with confidence.

Three steps to prevent being a victim:
PM Modi enumerated the three steps to ensure digital security.

- **STOP:**
  As soon as you get a call, stop. Don't panic, stay calm, don't take any hasty steps, don't give away your personal information to anyone; if possible, take a screenshot and record it for sure.

- **THINK:**
  No government agency threatens you on the phone; neither inquires nor demands money on a video call like this. If you feel scared, then know that something is wrong.

- **TAKE ACTION:**
  Dial the national cyber helpline 1930, report on cybercrime.gov.in , inform family and police, preserve evidence.

'Stop', then 'Think', and then take 'Action'; these three steps will become the protector of your digital security.

07

Appendices

- Useful Links and Contact Information

Useful Links and Contact Information:

- Secure Banking Page: *https://www.hdfcbank.com/personal/useful-links/security*
- Cybercrime Portal: *https://cybercrime.gov.in/* and Cybercrime Helpline Number: 1930
- Chakshu Portal: *https://sancharsaathi.gov.in/*
- RBI Kehta Hai: *https://rbikehtahai.rbi.org.in/*

Remember:
When you see a number starting with 1600 series, it's HDFC Bank safeguarding your transactions.

Your safety is our priority. Always pick up calls from 1600-series numbers. It's us, HDFC Bank.

Calls from 1600 series numbers are genuine. Responding to them helps us protect you from fraud.

HDFC Bank's transaction monitoring numbers are

1600 318475, 1600 313475
1600 308475, 1600 300475
1600 303475, 1600 310479
1600 318479

Always answer calls from these numbers.

Scan to follow **@vforvigilaunty**
to stay safe from financial fraud