## **Fraud Safety Suggestions from HDFC Bank:**

HDFC Bank consistently updates its security advisories on its website and through customer communications. Their advice typically covers:

**1. Protecting Your Personal and Financial Information:**

* **Never share sensitive details:** This is paramount. HDFC Bank (or any bank) will **NEVER** ask for your:
  + ATM PIN
  + Debit/Credit Card CVV
  + OTP (One-Time Password)
  + NetBanking IPIN (Password)
  + Customer ID
  + UPI PIN
* **Be wary of unsolicited communication:** Do not respond to calls, SMS, or emails asking for these details, even if they claim to be from the bank, RBI, government agencies, or any authority.
* **Destroy sensitive documents:** Shred or tear up any documents containing personal or financial information (account statements, credit card bills, pre-approved offers) before discarding them.
* **Update contact details:** Ensure your mobile number and email ID are always updated with the bank so you receive legitimate alerts.

**2. Secure Online and Digital Transactions:**

* **Always use official channels:**
  + **Website:** Always type [www.hdfcbank.com](https://www.hdfcbank.com) directly into your browser's address bar. Do not click on links in emails or SMS.
  + **NetBanking:** Ensure the URL starts with <https://netbanking.hdfcbank.com> and look for the padlock symbol. Use the virtual keyboard for typing passwords, especially on shared computers.
  + **Mobile App:** Download the official HDFC Bank MobileBanking app ONLY from official app stores (Google Play Store, Apple App Store).
* **Strong Passwords:** Use complex, unique passwords for your banking accounts. Change them regularly (e.g., every 3 months). Avoid easy-to-guess information like birth dates or names.
* **Public Wi-Fi caution:** Avoid performing financial transactions on public or unsecured Wi-Fi networks. If absolutely necessary, use a Virtual Private Network (VPN).
* **Beware of Phishing/Smishing/Vishing:**
  + **Phishing (Email):** Fake emails designed to steal your login credentials or other sensitive data. Look for generic greetings, grammatical errors, suspicious links, and urgent language.
  + **Smishing (SMS):** Fraudulent SMS messages with similar tactics. Do not click on links in suspicious SMS.
  + **Vishing (Voice Call):** Fraudsters posing as bank officials, government employees, or police to trick you into revealing details or performing actions (like downloading remote access apps). HDFC Bank advises calling their official PhoneBanking number (usually on the back of your card or their official website) if in doubt.
* **Review Account Activity:** Regularly check your bank statements, transaction history, and last login time for any suspicious or unauthorized activity. Set up HDFC Bank's "InstaAlerts" for real-time notifications.
* **Secure your devices:** Keep your computer and mobile devices updated with the latest operating system, antivirus, and anti-malware software. Avoid "rooting" or "jailbreaking" your mobile devices.

**3. ATM and Card Safety:**

* **Cover your PIN:** Always cover the keypad with your hand when entering your PIN at an ATM or POS machine.
* **Inspect ATM/POS:** Before using, check for any skimming devices on the card reader or suspicious cameras near the PIN pad.
* **Keep card in sight:** When making payments at stores or restaurants, ensure your card is swiped only on legitimate machines and remains in your sight.
* **Block lost/stolen cards immediately:** If your Debit or Credit Card is lost or stolen, block it immediately via NetBanking, Mobile Banking, or by calling HDFC Bank customer care.

**4. Money Mule Scams:**

* Be cautious of offers that seem too good to be true, especially those asking you to receive money into your account and then transfer it elsewhere, often with a commission. This is a common tactic for money laundering.

## **Fraud Safety Suggestions from RBI:**

The RBI, as the banking regulator, issues comprehensive guidelines and conducts awareness campaigns to protect customers. Their focus is on both bank responsibilities and customer vigilance.

**1. Zero Liability/Limited Liability in Unauthorized Electronic Banking Transactions:**

* **Report promptly:** The RBI's most critical guideline is to report any unauthorized electronic transaction *immediately* to your bank.
  + **Zero Liability:** If you report the unauthorized transaction within **3 working days** of receiving the communication from the bank regarding the transaction, you have zero liability, provided the loss is due to bank's negligence, third-party breach, or technology failure.
  + **Limited Liability:** If you report between 4-7 working days, your liability is limited based on the transaction type and amount. After 7 days, the bank's policy would apply, and your liability might increase.
  + This is a crucial consumer protection mechanism.

**2. Customer Awareness Campaigns (e.g., RBI Kehta Hai, BE(A)WARE):**

* The RBI runs various campaigns (like "RBI Kehta Hai" - RBI Says) to educate the public through TV, radio, and social media. These often highlight:
  + **Never share sensitive information:** Reiterating that RBI, banks, or government agencies *never* ask for PIN, OTP, CVV, passwords.
  + **Beware of Impersonation:** Fraudsters often impersonate RBI officials promising prizes, lottery winnings, or job offers in exchange for money. The RBI explicitly states it does not conduct such activities.
  + **Caution with unsolicited calls/SMS:** Emphasizing that official communications will not ask for sensitive data.
  + **Check website authenticity:** Always verify the website's URL and look for "https://" before entering any financial information.

**3. Regulatory Prescriptions and Institutional Safeguards for Banks:**

* Recent RBI circulars, especially on "Prevention of Financial Frauds Perpetrated Using Voice Calls and SMS" (January 2025) and integrating DoT's "Financial Fraud Risk Indicator (FRI)" (July 2025), mandate banks to:
  + **Utilize Mobile Number Revocation List (MNRL):** Banks must clean their customer databases and monitor accounts linked to disconnected/fraudulent mobile numbers to prevent their misuse as "money mules."
  + **Share Verified Customer Care Numbers:** Banks must share official customer care numbers with the Digital Intelligence Platform (DIP) for public display on "Sanchar Saathi."
  + **Use Specified Numbering Series:** Banks are required to use specific numbering series for commercial communications (voice/SMS) as per TRAI guidelines, making it easier for customers to identify legitimate communication.
  + **Enhanced Customer Awareness:** Banks must intensify awareness campaigns through multiple channels (email, SMS, vernacular languages) about fraud identification, DND registration, and recognizing trusted communications.
  + **Real-time Threat Detection:** Banks are mandated to use AI/ML-based tools like FRI to identify fraudulent activities in real-time, assign risk scores to transactions, and take proactive measures.
  + **Strong Authentication:** Banks must implement multi-factor authentication (MFA) for digital transactions and a risk-based approach to security, applying higher security for high-risk transactions.
  + **Transaction Alerts:** Banks must provide instant SMS and email alerts for all transactions.
  + **Cooling Period:** For new beneficiary additions, a cooling period (e.g., 30 minutes) is often imposed before funds can be transferred, allowing customers to detect and report unauthorized additions.

**Where to Find More Information:**

* **HDFC Bank "Beware of Fraud" section:**
  + <https://www.hdfcbank.com/personal/useful-links/security/beware-of-fraud>
  + This page often has detailed explanations of various fraud types (phishing, vishing, smishing, identity theft, money mule) and specific prevention tips.
* **HDFC Bank Security Measures/Guidelines:**
  + <https://www.hdfcbank.com/personal/useful-links/security/security-measures>
  + <https://www.hdfcbank.com/personal/resources/learning-centre/secure/safe-online-banking-tips-measures>
* **RBI's Consumer Education and Protection Department:**
  + <https://www.rbi.org.in/Scripts/bs_viewcontent.aspx?Id=2415> (General Consumer Education Page)
  + **"RBI Kehta Hai" Portal:** While not a direct static URL, search for "RBI Kehta Hai" on the RBI website for their campaigns.
  + **Press Releases and Notifications:** Keep an eye on the "Press Releases" and "Notifications" sections under the RBI website, especially from the Department of Regulation (DoR) and Department of Supervision (DoS), for the latest fraud-related guidelines.
  + **RBI's BE(A)WARE booklet/resources:** This resource often provides practical advice. Search for "RBI BE(A)WARE" on their site.

Always stay vigilant and remember the golden rule: **If it sounds too good to be true, or if someone asks for your sensitive banking details, it's very likely a fraud.**