



NEWS RELEASE

HDFC Bank Ltd.
HDFC Bank House,
Senapati Bapat Marg,
Lower Parel,
Mumbai - 400 013.
CIN: L65920MH1994PLC080618

HDFC Bank Shares an Important Message to Caution Citizens Against APK Fraud

Mumbai, August 05, 2025: HDFC Bank, India's largest private sector bank, advises customers to remain vigilant against APK (Android Package Kit) frauds. The aim is to increase awareness about such frauds to safeguard customers.

In an APK scam, fraudsters typically use social engineering tactics by impersonating bank employees or government officials. This involves the recipient of the message to receive a malicious APK file claiming to be from trustworthy sources. When a person installs these files, the fraudster gets full control of their phones. The fraudster can then redirect calls and text messages to another device and steal data from victims' phones. Fraudsters can also access victim's bank account(s) and carry out transactions without their consent.

How does this scam work:

1. Fraudsters typically impersonate government officials, employees of banks or well-known companies on the pretext of doing a Re-KYC, payment of traffic fines, refund of income tax, etc. A message is sent to the victim containing a fake APK link.
2. Once the victim clicks on the link, a malware gets installed on their mobile phone unknown to them.
3. This enables the fraudster to get full access to the victim's phone through this malware
4. Post this, typically within the next few minutes, multiple unauthorised transactions take place, causing financial losses to the customers. The victim realises that they have been duped upon receiving messages from their Bank about money being debited from their account.

Some examples:

- a. Fraudsters reach out to customers via phone calls, emails or messages claiming to be from the bank and their KYC needs to be updated immediately. They create a sense of urgency and fear of the account getting blocked. The fraudsters then share fake APK links which could be embedded with a bank logo and ask customers to install it. Once installed, the app prompts them to enter sensitive details like the person's account number, credit/debit card information or OTPs which are instantly stolen and misused for fraudulent transactions.

b. Fraudsters could also impersonate transport authorities (RTO) and send fake messages and emails related to a pending e-challan. These messages contain malicious APK links, and when clicked, compromise the victim's phone.

Tips to protect yourself from APK fraud

- Do not click on suspicious links or install apps / files received via social media, SMS, or email claiming to be from institutions like, the RTO, Income Tax Department, or Bank officials.
- Ensure your device has reliable antivirus or anti-malware software that can detect and block harmful files.
- Do not download third-party apps over a call request from an unknown person. Download apps only from trusted sources or official websites.
- Verify the legitimacy of the message / emails through the respective official website.
- Report fraudulent/suspicious calls, messages on the Chakshu portal at <https://sancharsaathi.gov.in/> or via the Sanchar Saathi mobile app.

HDFC Bank also urges customers to remain vigilant against scams, such as “digital arrest” fraud, where fraudsters impersonate law enforcement or government officials and threaten victims with a digital arrest warrant for reasons that could range from alleged tax evasion, regulatory violations, financial misconduct among others. Other frauds commonly seen include investment scams, where fraudsters promise unusually high returns on investments in stocks, IPOs, cryptocurrency, etc. via fake automated investment platforms and promoted via social media platforms. Fraudsters target the emotions of victims to perpetuate frauds by using the GTH – Greed, Threat and Help method.

In the event of falling prey to online fraud the victim should immediately report the unauthorised transactions to the bank in order to get the payment channel blocked, i.e., cards/UPI/net banking to safeguard against future losses. Customers should also file a complaint by calling **1930**, a helpline number started by the Ministry of Home Affairs (MHA) as well as submit a complaint on the National Cyber Crime Reporting Portal <https://www.cybercrime.gov.in>

About HDFC Bank

Please click here: www.hdfcbank.com