What is USB Debugging in Android?
Android USB Debugging is a helpful tool for developers, but it can also be risky. It lets someone with a computer control your phone in powerful ways. This means cybercriminals could potentially:

- Steal your information
- Install unwanted apps
- Alter and misuse with your phone's data

It's best to only enable USB Debugging when you absolutely need it, and only on trusted computers.

What does it mean for an Android device to be rooted?
Rooting your Android phone gives you more control, but it's risky! Here's why:

- Download bad apps: Rooting lets you bypass security safeguards, so you might accidentally install apps that steal your information.
- Easier hacking: Rooting makes your phone more vulnerable to attacks, hackers could take complete control.
- Lose security features: Rooting might disable some of your phone's built-in protections.

What does it mean for an iPhone to be jailbroken?
Jailbreaking an iPhone means bypassing iOS security restrictions, leaving it vulnerable to malware and hackers. This can lead to data theft, including passwords, and full access to the device. Jailbreaking also disables iOS security features.

What does 'Screen Mirroring' or 'Screen Casting' mean?
Screen mirroring lets one device display what's on another device's screen. However, it poses risks as fraudsters could access sensitive data like CVV numbers, OTP details, and passwords, potentially leading to stealing money from your account.

What does 'Screen Recording' mean?
Screen recording is capturing a video of your device's screen activity, either using the device's built-in camera or specialised apps.
However, it poses risks as fraudsters could access sensitive data like CVV numbers, OTP details, and passwords, potentially stealing your hard-earned money.

What does 'Screen Sharing' mean?
Screen sharing displays your screen to other devices and fraudsters may take control of your device. Risks include:

- Untrustworthy apps stealing personal data.
- Malware accessing sensitive info for fraud.
- Fraudsters exploiting shared screens for theft.

What is a 'Hooking Framework'?
Hooking frameworks are tools utilised by attackers to modify how applications or systems operate. Here's how they work:

- "Hooking" alters application or system behavior.
- Attackers use hooking frameworks to intercept and modify function or API calls.
- This grants control over program execution, allowing redirection to malicious code.
- Malware leveraging hooking frameworks can steal sensitive data like login details, passwords,

and payment information.
- It can also monitor and intercept data flows to and from mobile devices.

What is a 'Java Debugger'?
The Java Debugger (JDB) is a tool for Java programmers to fix issues in their programs. However, it can also be misused:

- Attackers can exploit JDB to gain access to systems, potentially causing damage.
- Specifically, attackers may use JDB to access bank servers through specific ports.

What is Malicious or Risky Software, Program, or App?
Malicious or risky software, programs or apps aim to harm devices or networks. Risks include:

- Theft of sensitive data (login details, passwords, payment information).
- Misuse of data for stealing money.
- Attackers gaining access to bank servers via specific ports if malware is present.

What is 'Unsecured Wi-Fi'?
Unsecured Wi-Fi is any network you can join without a password. These networks are dangerous because they lack security features that protect your information from hackers.

Is it safe to use unsecured Wi-Fi?
Unsecured Wi-Fi can be risky! Hackers might steal your information or infect your device without you knowing. This is because public Wi-Fi often lacks security.
Stay safe: Use only secured Wi-Fi networks, especially for things like banking.

What is additional authentication, and why is it necessary for certain transactions?
HDFC Bank uses AI to watch out for risky transactions. Depending on the risk, your transactions might require:

- No extra step: Just swipe on the 'Pay' button.
- A PIN or code: Enter your mPIN or a one-time code.
- Extra verification: Provide both a code and additional info for certain transactions.

Why are certain transactions declined after authentication for security reasons, and what should I do in such cases?
We understand this can be confusing, but rest assured, your account is safe.
Your security is our top priority. We use advanced Artificial Intelligence (AI) to detect and prevent potentially risky banking activities.
To protect you, we sometimes decline transactions that seem suspicious. If a genuine transaction is declined, please contact HDFC Bank customer care at 1800 1600 / 1800 2600. We're here to help.

Why is authentication not required for certain transactions, and why are 'Swipe to Pay' transactions confirmed without authentication?
For transactions below a specified amount, users do not need to enter their mPIN for authentication. Simply swiping on the 'Pay' button confirms the transaction, and the funds are immediately transferred.
For such transactions, we will show you on screen that no other authentication is required.