Title:

Mobile Banking Malware: SOVA Android Trojan

Dear Valued Customers,

This malware hides itself within fake Android applications that show up with the logo of a few famous legitimate apps like Chrome, Amazon and NFT (Non-fungible Token) platform to deceive users into installing them. This malware captures the credentials, when users log into their net banking apps and access their bank accounts.

The malware is capable to perform the following functions:

- Collect keystrokes
- Steal cookies
- Intercept multi-factor authentication (MFA) tokens
- Take screenshots and record video from a webcam
- Perform gestures like screen click, swipe etc. using android accessibility service
- Copy/paste
- Adding false overlays to a range of Apps
- Mimic over 200 banking and payment applications

Best Practices and Recommendations:

1. Download Apps from official App stores (*Play Store* for Android and *App Store* for iOS).
2. Install Android updates and patches as and when available from Android device vendors.
3. Install and maintain updated anti-malware and anti-spyware software.
4. Be cautious for suspicious numbers that don't look like real mobile phone numbers. Genuine SMS messages received from banks usually contain sender id (consisting of bank’s short name) instead of a phone number in sender information field.
5. Only click on URLs that clearly indicate the website domain.
6. Look out for valid encryption certificates by checking for the green lock in the browser's address bar, before providing any sensitive information.

Report fraud immediately to your Branch or Call on our toll free No. 1800 103 1906.

For calling your Branch, always use numbers available on your passbook, account statement or on Bank’s Website https://bankofindia.co.in → locate us → Branches.

Report cyber frauds also on Government of India portal – https://cybercrime.gov.in/ or Call on 1930

आदर एवं आभार सहित /Thanks & Regards,

बैंक ऑफ़ इंडिया
Bank of India BOI

Information Security Team