Beware of SMS Spoofing using Android Malware targeting UPI Apps

Cybercriminals have been exploiting a weakness related to SMS spoofing, which allows them to potentially gain control over victims' UPI accounts by circumventing the device binding process. Device binding is a crucial step that ensures the registration of a trusted device for banking purposes.

To carry out these attacks, cybercriminals are utilizing various methods by leveraging native platforms. They may create customized Android payloads with deceptive names like "Hospital Appointment," "Hotel Booking," or "Courier Delivery Assistance" (e.g., courier.apk). These payloads are designed to redirect the UPI app's device binding message to a Virtual Mobile Number (VMN) associated with the victim's bank for fraudulent registration.

It is crucial for users to remain cautious and adopt necessary security measures to safeguard their UPI accounts and personal information.

Modus Operandi

⇒ Fraudster initiate contact with target users who seek online assistance through search engine for services like courier delivery, hotel booking, hospital appointment etc.

⇒ Malicious APK (Android package) file is sent by fraudster via instant messaging platform like WhatsApp, Telegram etc.

⇒ The malware, once installed on the victim's device, is hardcoded to forward incoming SMS messages to a virtual mobile number associated with the fraudster's bank.

⇒ Fraudster initiate the UPI registration (device binding) process on behalf of the victim. As part of this process, the UPI app sends a registration SMS to the victim's device.

⇒ The malicious APK intercepts the registration SMS and forwards the SMS to the Bank for completing the UPI registration process. This action binds the fraudster's phone to the victim's UPI app or account.

⇒ After binding the UPI app with fraudster's phone, the fraudster employs social engineering techniques to trick the victim into revealing UPI credentials like UPI PIN, MPIN, TPIN etc. for performing fraudulent/unauthorized UPI transactions.

Security Best Practices

✗ Avoid installing apps from unknown sources like clicking on .APK / .EXE files or third-party app stores or at the behest of any stranger.

✓ Download apps only from reputable trusted sources.

✓ During installation, carefully review the permissions requested by the app. Never grant unnecessary permissions to Apps.

✓ Regularly update device operating system and UPI apps to ensure the latest security patches and bug fixes are installed.

✓ Install reputable Antivirus / antimalware solution and perform regular scanning for any potential threats.

✗ Avoid clicking on unknown links received via SMS, Emails, instant messaging platforms, social media etc.

✓ Use strong passwords / pattern lock / biometric authentication to lock both the UPI app and device & also enable two-factor authentication as additional layer of security.

✓ Regularly monitor your UPI transactions for any unauthorized or suspicious activity. If any suspicious transaction is noticed, report to your Bank / Branch immediately.

✗ Never share UPI credentials, MPIN, TPIN or any sensitive information with anyone under any circumstances and avoid saving passwords, PIN etc. in devices.

Report Cyber fraud Incidents to https://www.cybercrime.gov.in or Call 1930 for assistance

यूको बैंक UCO BANK
(भारत सरकार का उपक्रम) (A Govt. of India Undertaking)
सम्मान आपके विश्वास का Honours Your Trust

CISO OFFICE

Security Advisory 102 dated 24.05.2023