Security Advisory: Beware of "APK" Mobile Application Fraud

Nowadays, Cybercriminals are using various tactics, including manipulation through downloading unverified Applications into mobile device to gain unauthorized access to personal or sensitive information for conducting fraudulent activities.

Modus Operandi

- Fraudsters posing as government officials often contact individuals under false pretenses like updating of PAN Card, Aadhaar Card, KYC etc.
- Individuals are then directed to download unverified Applications like ".APK" or ".EXE" files etc.
- Once the malicious files / Apps are downloaded, cybercriminals may gain access to the device, enabling them to read messages containing sensitive financial information like OTP, PIN etc.
- Taking full control of the victim's device, cybercriminals are able to conduct unauthorized online transactions, fund transfers to anonymous account etc. from victim's Bank account.

Cyber Safety Best Practices

Do's

- ✓ Always use official channels for any updates or services related to government IDs or Banking matters.
- ✓ Download apps only from verified and trusted sources such as Google Play Store, Apple App Store etc.
- ✓ Frequently review App Permission Setting & grant only those permissions which are utmost necessary.
- ✓ Keep your device's operating system and apps updated with latest patches & fixes.

Don'ts

- ✗ Avoid third-party Apps or links shared over unsolicited calls / messages / instant messaging platforms like WhatsApp, Telegram etc.
- ✗ Avoid downloading Apps from unknown sources or unfamiliar links.
- ✗ Never grant unnecessary permissions to Apps which allow remote access.
- ✗ Be cautious of unexpected calls / messages asks for sharing sensitive information.

Report Cyber fraud Incident to https://www.cybercrime.gov.in

or call 1930 for assistance