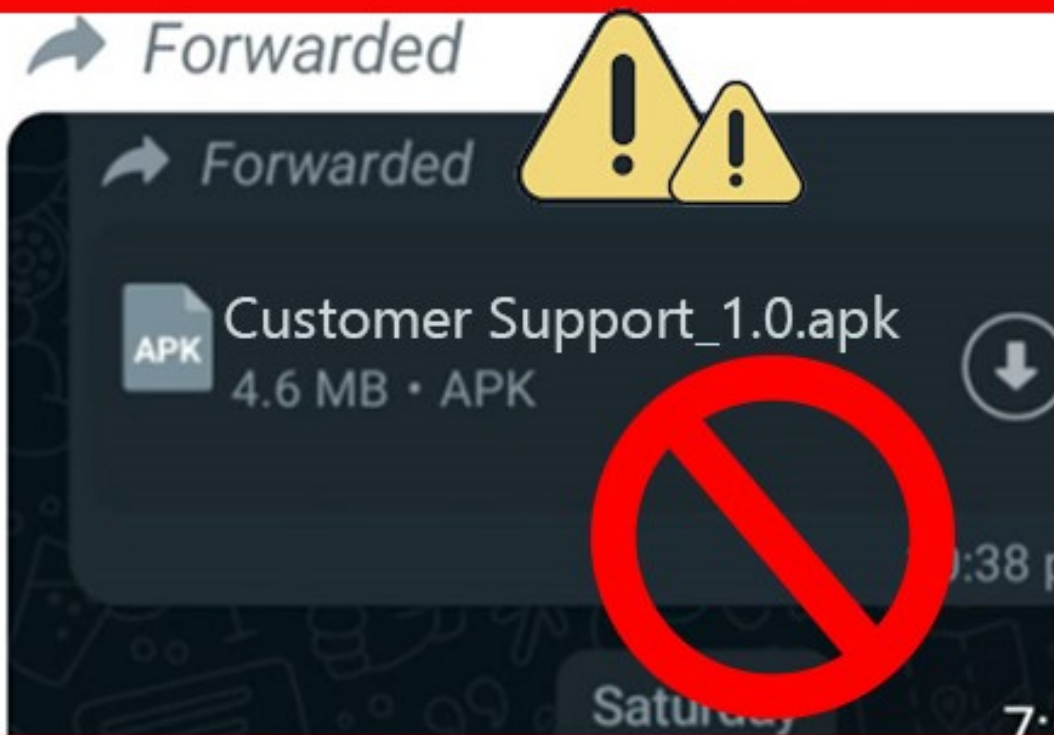




Beware of random files with .APK extension



Nowadays, cybercriminals are circulating malicious files with **.apk** extension through WhatsApp to dupe unsuspecting individuals.

Modus Operandi of the Scam

- ➔ Cybercriminals target users through messaging platforms like WhatsApp.
- ➔ Victims receive messages containing files with .apk extensions from unknown or suspicious numbers.
- ➔ Upon clicking or downloading the file, a malicious App is getting installed on user's device silently in the background.
- ➔ The rogue App operates covertly, running without the user's knowledge.
- ➔ The App may possess capabilities to intercept calls, messages, or even grant remote access to the device.
- ➔ Cybercriminals exploit this access to commit financial fraud or steal sensitive information for nefarious purposes.

How to Stay Safe

- ✗ Refrain from downloading or clicking on files sent by unfamiliar contacts.
- ✗ Never download unexpected files with malicious extensions like ".APK", ".EXE" etc.
- ✗ Do not forward or share unknown files, rather delete the message.
- ✓ Activate security features on device such as "Disable Auto Download" settings to prevent auto downloading of files from untrusted sources.
- ✓ If you encounter suspicious messages, files or activity on WhatsApp or any other platform, report it immediately to the platform's support team or relevant authorities.
- ✓ If received suspicious communication via calls, SMS or WhatsApp, report such numbers immediately to Govt's **CHAKSHU Portal** at <https://sancharsaathi.gov.in> to prevent cybercrime & financial fraud.

