Community Advisory:

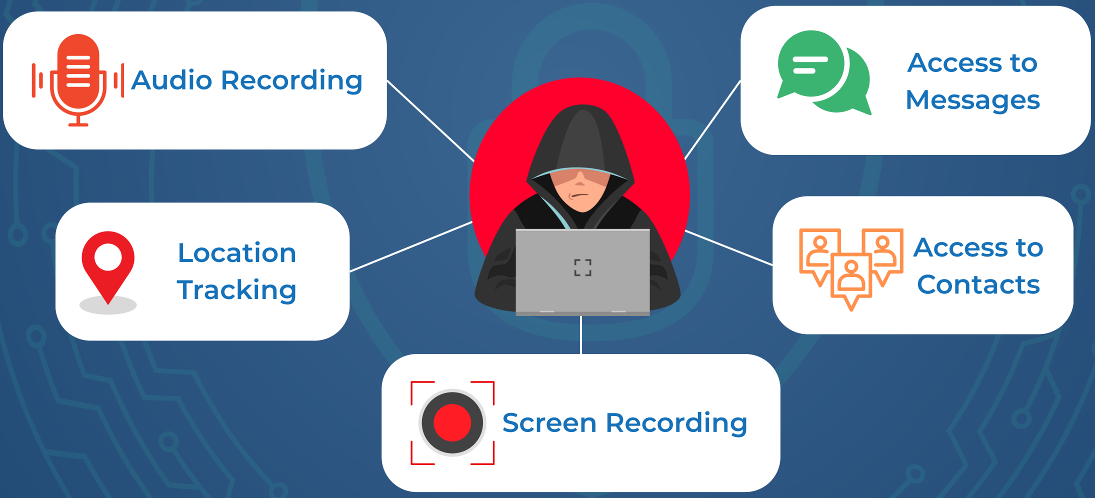
Protecting Against Spoofed Apps & Mobile Spyware

What's Happening?

Recent analysis by the UK's National Cyber Security Centre (NCSC) and international partners has revealed the continued use of **spyware campaigns** targeting Tibetans, Uyghurs, and Taiwanese communities. These campaigns rely on **spoofed apps** — fake or modified versions of legitimate apps — where the original app has been tampered with and infected with malware, then **distributed as trusted** tools. These apps are often disguised as culturally relevant resources such as religious, language, or communication tools, making them appear safe while silently compromising user devices.

If you download an app from a link or site with malicious code embedded in the app "package" or "APK" you may also unknowingly download spyware.

Two variants of spyware, BADBAZAAR and MOONSHINE have been confirmed to:



Audio Recording

Access to Messages

Location Tracking

Access to Contacts

Screen Recording

Apps Targeted by Spyware Campaign

Important: The Apps listed in this advisory were **spoofed by attackers** - this does not mean the original apps are harmful

- Tibetan Prayer
- Singing Bowl Sound HD
- 藏历基本数据
- Tibetan Divination App (MO)
- 阳光藏汉翻译
- Telegram
- Signal
- WhatsApp
- Zom Messenger

Tibet Action Institute
བོད་དོན་ལས་འགུལ་བསྐྱི་གནས་ཁང་

TIBCERT

Verified Developers and Origins of Flagged Apps

App	Developer	Origin
Utility Apps		
Tibetan Prayer	Tibetan Computer Resource Centre (TCRC)	CTA
Signing Bowl Sound HD	Sound Jabber	US
Tibetan Divination System Mo	Rhomb Apps	US
藏历基本数据(Tibetan Calendrical Data)	西藏自治区藏医院	China
汉藏英辞典(Chines-Tibetan-English Dictionary)	成都遇欢喜文化传播有限公司	China
阳光藏汉翻译 (Sunshine Tibetan-Chinese Translation)	西藏大学信息化研究所	China
Messaging Apps		
Signal	Signal Foundation	US
Zom	Zom	US
Telegram	Telegram FZ-LLC	Dubai, UAE
WhatsApp	WhatsApp LLC	US

- On the left, we have provided a list of verified developer names for Tibetan apps that were flagged in our advisory.
- If the app installed on your device shows a different developer, it is potentially a spoofed or malicious version.
- In that case, we strongly recommend following the steps on the next slide on how to protect yourself and secure your device.

Key Details to Watch Out For:

- Apps like (Tibetan Prayer, Singing Bowl Sound HD, 藏历基本数据 (Tibetan Calendrical Data), 汉藏英辞典 (Chines-Tibetan-English Dictionary), Tibetan Divination System Mo, 阳光藏汉翻译(Sunshine Tibetan-Chinese Translation)) aren't on app stores and require sideloading.
- Sideloaded apps may offer features but lack security audits, posing serious risks.
- They don't get regular updates, making them vulnerable to bugs and exploits.
- Check an app's country of origin and data protection policies before installing.

Tibet Action Institute
བོད་དོན་ལས་འགུལ་བསྒྲི་གནས་ཁང་

TIBCERT

How to Protect Yourself - Checklist to Spot Spoofed Apps

1.Check App Details:

- Check Developer’s Info
- Check out Ratings and Reviews
- Check App Privacy and Data Safety
- Check Developer website for more information
- Check the credibility of the company/app developer

2. Examine the App’s Name and Icon Carefully

- Is the name spelled slightly differently? (“Tibetan Paryer” instead of “Tibetan Prayer”)
- Is the logo low-quality or slightly altered?
- Spoofed apps often copy real ones but make small visual/textual changes.

3. Look at Permissions

- Review permissions before installing an app
- Only allow what’s necessary for the app to work
  - For example: A Tibetan calendar app doesn’t need access to your location or microphone - turn these off.

4. Scan the APK (for Android Apps)

If you download an app file (APK), use:

- VirusTotal.com – Upload the file and check if it's flagged
- Mobile Verification Toolkit (MVT) – For advanced users to scan devices for spyware
- Check the SHA256 hash of the file and compare it to the trusted one (if known)

What to Do If You Think You’ve Installed a Spoofed App?

1. Disconnect from Wi-Fi and mobile data

2. Uninstall the app immediately

3. Backup important data

4. Consider resetting your phone after backing up personal data

5. Reach out to TibCERT:

support@tibcert.org

WhatsApp: +91 8218207324

Or

Scan this to chat with us anonymously

Tibetans have long been at the forefront of unprecedented targeted digital attacks. Since first being reported in 2019, this mobile spyware campaign has continuously evolved—adapting new tactics to exploit our community’s habits and tools. It’s more important than ever to stay vigilant and protect our devices by following digital security best practices.

Stay alert. ⚠
Share knowledge. 📢
Secure your phone 🔐

Tibet Action Institute
བོད་དོན་ལས་འགུལ་བསྒྲི་གནས་ཁང་

TIBCERT