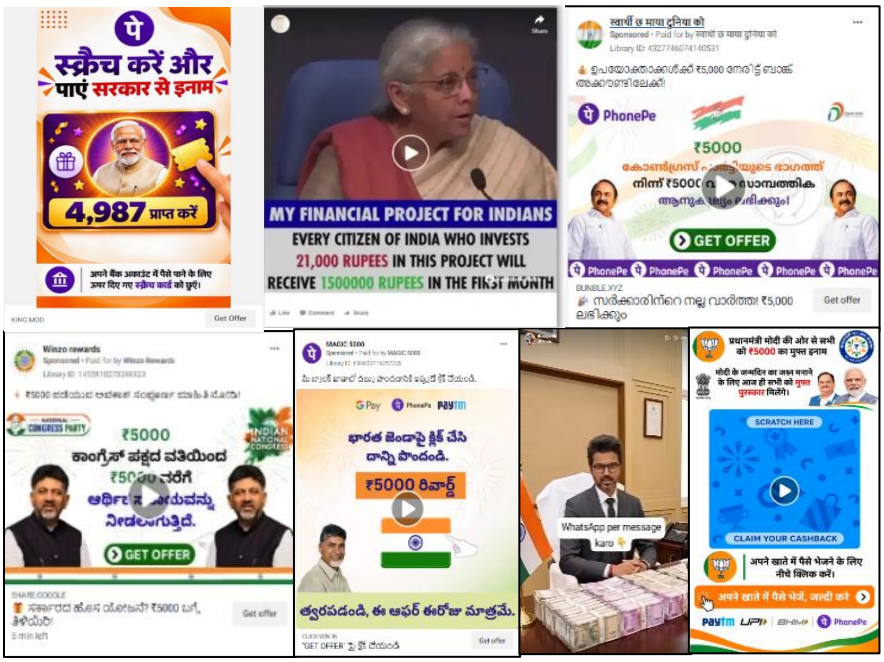
ADVISORY

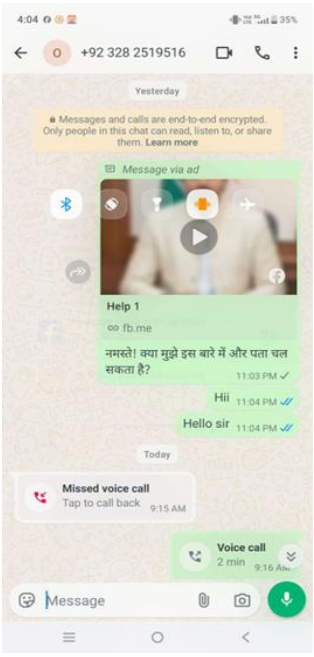
TAU/ADV/019 | Dated 19st October, 2026

Rise in Chief Minister / Public Figure Impersonation Scams - Promoting Welfare Schemes & Cashback Frauds Through Social Media Advertisements

The National Cybercrime Threat Analytics Unit (NCTAU) has observed rise in financial fraud through deceptive advertisements on Facebook and Instagram. These advertisements impersonate well known public and political figures, including the Prime Minster of India, the Finance Minister, Chief Ministers of States, to promote fake Government welfare schemes and promise financial assistance. Victims are asked to pay purported fees or taxes to receive the benefits. In some cases, advertisements offer fake cashback rewards through scratch-card or spin-and-win contests, tricking victims into approving UPI collect requests from fraud merchants and transferring money to fraudsters.

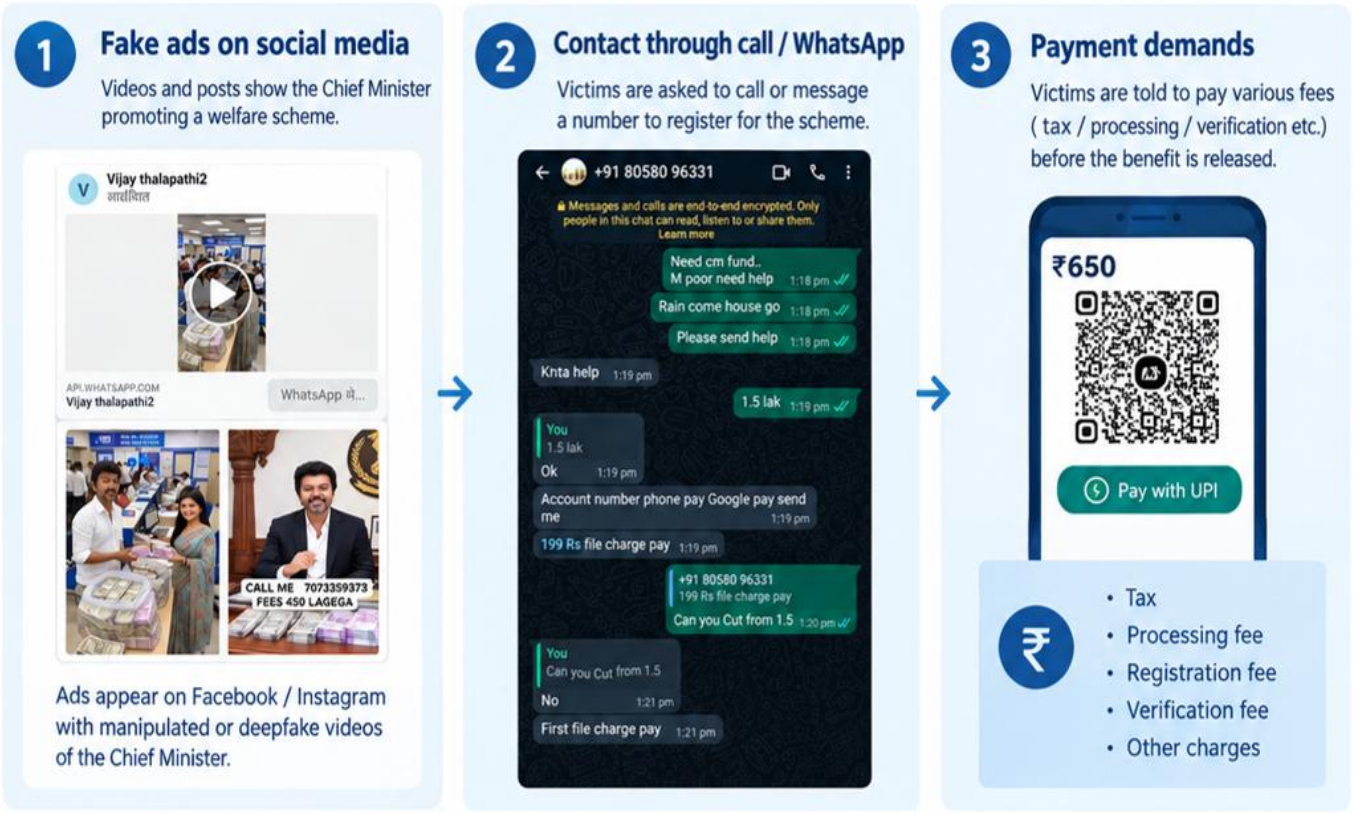


Social Media Advertisements Impersonating the Political Figures

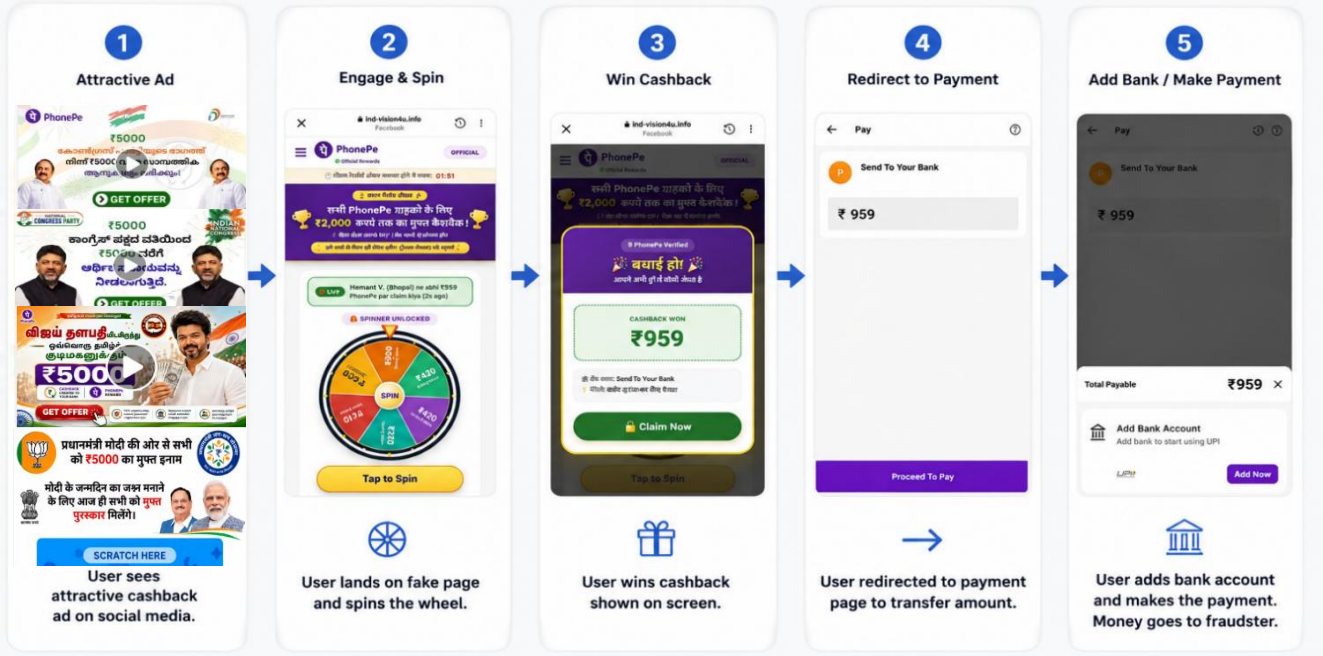


Call / message from +92 WhatsApp Account

If any Public figures or their offices contact you from +92 (Pakistan) numbers, treat such calls with extreme caution and refrain from engaging.



Public Figure Impersonation – Fake Government Scheme/Yojna



Scratch Card/Spin-and-Win: Cashback Fraud

MODUS OPERANDI

1. **Distribution:** Ads, majorly on Meta Platforms featuring manipulated/deepfake videos ostensibly show the public public figures announcing and promoting a welfare scheme allegedly intended to provide financial assistance to the needy. The advertisements containting phone numbers either offer financial assistance under a purported welfare scheme or cashback/rewards through scratch-card or spin-and-win offers. Many of the websites fall under the category of Political advertisements.

2. **Initial Contact & Victim Engagement**: Victims are either directed to a phone number/WhatsApp chat or redirected to a fraudulent website through the advertisement in order to claim the funds/benefits of the purported scheme. In many instances, victims receive calls from international numbers, majorly Pakistan based (+92 numbers) claiming that they have been randomly selected to receive the alleged funds. In some instances victims are redirected to a website which contains a scratch card or spin and win.

3. **Advence Fees**: Victims are coerced to make repeated payments under the pretext of taxes, processing fees, registration charges, verification fees or other administrative expenses in order to receive the funds and benefits.

4. **Financial Fraud**: Victims make multiple payments and suffer substantial cumulative financial losses. In some instances, the vicitms are redirected to a payment app and induced to enter their transaction PIN on the pretext of receiving the prize money. The transaction, however, results in money being debited from the victim’s account and transferred to the perpetrator.

PRECAUTIONS AND SAFETY RECOMMENDATIONS

1. **Verify Welfare Schemes:** Before acting on social media advertisements, check details of welfare schemes on the official website of the concerned department.
2. **Check Payment Requests:** Verify the purpose and recipient of any fee or payment requested in connection with a welfare benefit.
3. **Verify Identity:** Confirm the identity of persons claiming to represent Government departments through official channels. In case of any doubt, visit office in person.

4. **Protect Personal and Financial Information:** Exercise caution when sharing Aadhaar, PAN, bank details, OTPs or UPI PINs with unknown persons.
5. **Check Video Authenticity:** Treat videos and voice recordings featuring public officials with caution and verify the claims through official sources.
6. **Review UPI Requests:** Before approving a UPI collect request or entering a UPI PIN, check the transaction details. A UPI PIN is used to authorise payments, not to receive money.

Report any fraudulent applications or any scam incident immediately on **1930** or **www.cybercrime.gov.in**