ADVISORY

TAU/ADV/007 | Dated 04th Dec 2025

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

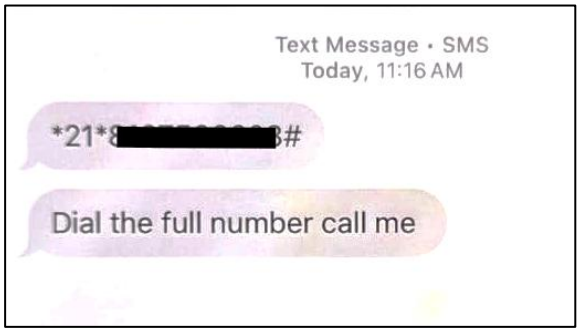
Indian Cyber Crime Coordination Centre

USSD based call forwarding scam – Delivery agent impersonation

The National Cybercrime Threat Analytics Unit of I4C has observed a trend in cybercrime where USSD (Unstructured Supplementary Service Data) code is being used to enable call forwarding by impersonating Delivery Agent. A USSD is a special sequence of numbers, asterisks "*****"and hashes " # " used to interact with Telecom Service Provider or access telecom services without needing an internet connection.

MODUS OPERANDI

- It has been observed that cybercriminals are impersonating delivery or courier service agents and contacting citizens under the pretext of confirming or rescheduling deliveries.
- Victims are then instructed to dial codes sent via SMS that begin with ***21*,** followed by a mobile number (belonging to fraudster).
- Dialing such USSD code automatically activates call forwarding on victim's mobile phone. This results in calls from banks, payment OTP verifications, or authentication codes of WhatsApp / Telegram etc automatically redirecting to the fraudster's phone number.



Scammer convincing victim to enable call forwarding through USSD

- This results in unauthorized financial transactions as well as WhatsApp / telegram account hacking.

PRECAUTIONS

- **Do Not Dial** or enter any USSD code beginning with *21*, *61*, *67*, or similar prefixes shared by unknown callers.
- **Deactivate all forwarding**: In case call forwarding is activated, dial **##002#**, will instantly cancel all call forwarding services (busy, unreachable, no-answer).
- **Do Not Click** on suspicious courier or delivery links received via SMS, WhatsApp, or email.
- **Verify Delivery Details** directly with official courier services through their website or customer care helpline.
- **Report** any fraudulent applications or any scam incident immediately on **1930** or www.cybercrime.gov.in