Smishing Triad

[/ˈsmɪʃ.ɪŋ ˈtraɪ.æd/]

The Smishing Triad is a high-risk, financially motivated cybercrime group active since 2022, operating smishing-as-a-service campaigns. It targets consumers via postal, banking, and government lures, using advanced kits with OTP theft and mobile malware across the Middle East, South Asia, and North America.

IDENTITY

Attribution : Transnational cybercrime syndicate operating a smishing/phishing-as-a-service ecosystem; East/Southeast Asia nexus with regional affiliates.

Active Since : ~2022; marked expansion through 2024–2025.

Aliases : Uses shared “fraud kits” and reseller channels; multiple crews operate under the broader moniker.

Motivation : Monetization of stolen PII/payment data, account takeovers, and scaled fraud.

TTPs

Initial Access : Mass SMS lures impersonating postal, police, and banking brands; localized language/currency; shortened links; QR-based variants.

Execution : Phishing pages harvest card data, PII, and OTPs; Android APK droppers disguised as tracking apps; JS anti-bot to evade scanners.

Persistence : Follow-on contact via SMS/calls to extract additional info; recurring lure waves reusing victim numbers; account session hijack.

Command & Control (C2) : Real-time exfil via Telegram bots/webhooks; APIs post captured fields to operator panels; fast-flux hosting/CDNs.

Malware & Tools : Android info-stealers/SMS readers, web phishing kits (USPS, India Post, Egypt Post, Dubai Police themes), kit admin panels, OTP relays.

Techniques : Brand impersonation, MFA/OTP interception, device fingerprinting checks, geo/IP filtering, domain rotation and bulletproof hosting.

TARGET PROFILE

Sectors : Postal/logistics, financial institutions, telecom carriers, government service portals.

Geographies : UAE and wider GCC; Egypt/North Africa; India/South Asia; U.S. (USPS-focused); spillover to other regions via affiliates.

Victims : Consumers and SMB owners; high mobile usage populations; users awaiting deliveries or responding to fines/fees.

THREAT ASSESSMENT

Risk Level : High — scalable outreach, rapid kit duplication, real-time OTP theft increases likelihood of account takeover and fraud losses.

Most Recent Activity : 2024–2025 postal/banking waves in UAE/Egypt/India/U.S.; increased AI-aided localization and automation.

Evolution : More sophisticated kits (anti-bot/anti-scan), APK distribution for SMS interception, tighter mule recruitment and crypto cash-out.

NOTABLE OPERATIONS

- **USPS-themed waves (2024–2025):** U.S. consumers targeted with fee/verification lures; payment/identity theft at scale.
- **India Post smishing (2024):** Cloned pages capturing Aadhaar/KYC and card data; iPhone/Apple ID-themed cross-lures observed.
- **Dubai Police impersonation (2024):** Fake fines/penalties to coerce payment credential submission across UAE.
- **Egypt Post & financial lures (2024–2025):** Localized brand spoofing and Hong Kong/EU-hosted kits used for regional campaigns.