TrustGH
+233 20 241 7018 www.trustgh.com info@trustgh.com North Legon – Ghana ECOWAS Road
@TrustGh

PRESS RELEASE

TrustGH records more than 6,000 'scam' numbers as TikTok emerges a major fraud channel

Accra, Ghana — August 31, 2026

TrustGH, a scam verification and reporting platform, has identified more than 6,000 telephone numbers associated with suspected fraudulent activity through community reporting and open-source intelligence (OSINT) investigations conducted by its team of certified cybersecurity professionals.

The findings highlight the evolving digital fraud threat landscape in Ghana, with threat actors increasingly exploiting social media platforms, messaging applications, online business directories, telecommunications channels and fraudulent websites to target individuals and businesses.

TrustGH's analysis shows that approximately 50 per cent of reported scam numbers are linked to TikTok, making it the largest identified source of reported scam activity within the platform's database. SMS and WhatsApp also account for a significant proportion of reported cases, while other indicators have been traced to Facebook, Google Business Profiles, telephone calls and fake websites.

Social engineering driving digital fraud

TrustGH's investigations indicate that many of the identified schemes rely heavily on social engineering techniques rather than sophisticated technical exploitation.

Threat actors often impersonate trusted individuals or organisations to establish credibility and manipulate victims into transferring funds or disclosing sensitive information.

Fraudsters may pose as bank officials, government representatives, company executives, police officers, financial agents, recruitment officers or legitimate business owners.

Once trust has been established, victims may be pressured to make payments, disclose one-time passwords (OTPs), provide Mobile Money credentials or reveal other sensitive information.

These tactics can lead to financial loss or account compromise without the attacker necessarily gaining direct technical access to the victim's device.

Mobile Money remains the primary target

More than 90 per cent of reported scam cases analysed by TrustGH involved attempts to obtain Mobile Money payments or gain unauthorised access to victims' Mobile Money accounts.

The platform has identified several recurring threat categories, including Mobile Money fraud, financial impersonation, fake online sellers, fraudulent Google Business Profiles, fake recruitment schemes, prize and lottery scams, social-media fraud, suspicious callers and phishing-related account takeover attempts.

In phishing and account-takeover schemes, threat actors attempt to harvest authentication credentials, OTPs, passwords or other information that could enable unauthorised access to victims' accounts.

TrustGH considers the high proportion of Mobile Money-related incidents a significant cybersecurity concern given the widespread use of mobile financial services in Ghana.

Fake business profiles used as attack infrastructure

TrustGH has also identified a growing pattern involving the abuse of legitimate business identities.

Threat actors create fraudulent social-media accounts, advertisements and Google Business Profiles that closely imitate genuine companies.

These fraudulent profiles may reproduce legitimate business names, logos, locations and other publicly available information to create an appearance of authenticity.

TikTok a major source of reported scam indicators

The finding that approximately half of the reported numbers are associated with TikTok highlights the increasing role of social media in the fraud ecosystem.

Threat actors can use social platforms to establish fraudulent identities, advertise fake products or services and reach large numbers of potential victims.

Communication may subsequently move to WhatsApp, SMS or telephone calls, where social-engineering techniques are used to complete the fraud.

This creates a multi-channel attack chain in which several platforms may be used during different stages of the same scam.

Collaboration with cybersecurity and law-enforcement authorities

TrustGH is a licensed platform and works closely with the Cybersecurity Authority and the Cyber Crime Unit of the Ghana Police Service to combat scam activity and support investigations involving reported numbers.

Members of the public can verify and report suspicious numbers through **TrustGH.com**.

Visit: TrustGH.com

Issued by:
TrustGH
Public Scam Verification & Reporting Platform
Accra, Ghana