Joint Advisory on Social Media Cyber Threats and Scams in South Sudan

---

Official Press Statement

Juba, South Sudan—September 24th, 2024. In recent years, South Sudan has witnessed a significant increase in the use of social media platforms. This is due to both internet and mobile telecommunication penetration in the country. However, while these platforms offer numerous benefits in terms of communication and information sharing, the platforms also pose significant cyber threats and scams to users.

In South Sudan, Facebook and WhatsApp platforms appeared to be the most common grounds for cyber threats and scams being largely perpetrated by anonymous online actors. These threats come in the form of phishing attacks disguised as legitimate messages and links yet malicious to trick users into revealing sensitive information, and malware attacks where links or file attachments embedded with viruses and ransomware infect users' devices and compromise their data upon clicking and downloading.

Besides, cyber scams in South Sudan's digital environments, specifically social media platforms, have been fronted in terms of fake free giveaways, job and investment opportunities, scholarships, and so on, in a manner of impersonating credible individuals and both private and public institutions.

We established that these anonymous actors use social engineering tactics to exploit the psychological vulnerabilities of the victims and weak security features of their social media

accounts to hack or compromise them. As a result, several people fell victim to such tactics, including public figures, celebrities, and individuals.

These cyber threats and scams have compromised various social media users' accounts, especially on Facebook, which led to identity theft, where individuals' personal information is stolen and used fraudulently, and the release of private information (nude videos or photos) in the public domain without users' consent.

Given that, SafetyComm has documented 854 incidents of compromised social media accounts of users due to these fraudulent cyber threats and scam activities in the South Sudan digital environment or space from 2021 to 2024. Out of this, 460 accounts were recovered after the victims sought the support of SafetyComm. However, 327 accounts were unrecovered due to the victims' total loss of their account credentials or unwillingness to cooperate with our response team. Meanwhile, 67 cases were already worked on but still pending recovery.

Out of the social media platforms, 57.3% of the cyber threats and scam incidents were recorded from Facebook users, 22.8% from WhatsApp, 18.9% from Instagram, 0.9% from Telegram, and none from X, formerly Twitter.

Therefore, today's joint advisory on cyber threats and scams serves to alert the general public and social media users in South Sudan about ongoing inauthentic false alarms regarding Facebook page verification, community standards violations, and copyright infringement with threats to shut down users' accounts.

This comes after several people received notification messages either directly in their social media inboxes or through emails informing them allegedly from the Meta or Facebook support team about acceptance to start verification of their Facebook pages or profiles through malicious links, violation of Community Standards with phishing links to request an appeal, and infringement of copyrights.

The false alarm notification messages appear to urge the users to act urgently within a timeframe of 24 hours; if not, they would lose the opportunity to verify their Facebook page or profiles and accounts shut down in case of violations. As such, it is the exact tactics used by the anonymous actors to exploit social media users to compromise their accounts.

However, it appears that these messages are not directly from Meta but from individuals impersonating Meta or Facebook. The public is urged to pay attention and avoid clicking links attached to messages they receive, whether through email or direct messages in their social media accounts before they can verify.

With the cybercrime and computer misuse bill being processed by the national parliament to become a remedy to address cyber-related crime, law enforcement agencies, especially the police, also need to be empowered and bolstered to handle cyber fraud and exploitation in the digital environment in South Sudan.

By Nelson Kwaje, Team Lead