Singapore Threatens Meta With Fines Over Facebook Impersonation Scam

Data: 2025-09-27 00:07:37

Autor: Inteligência Against Invaders

The Singapore government has given Meta Platforms until September 30 to introduce measures to

curb impersonation scams on Facebook.

On September 24, the Singapore Police Force (SPF) issued an implementation directive addressed to the tech giant.

The directive was made public the next day on the country's Ministry of Home Affairs (MHA) website.

The SPF's Online Criminal Harms Act (OCHA) Competent Authority urged Meta to put in place measures to target scam advertisements, accounts, profiles and/or business pages impersonating key government office holders on Facebook.

These measures fall into two categories:

- Enhanced facial recognition measures for Singapore users
- Prioritizing review of end-user scam reports from Singapore

If Meta does not comply by September 30 and cannot show a "reasonable excuse" for its non-compliance, Meta risks paying a fine of up to S$1m (US$776,639) as well as a further fine of up to S$100,000 (US$77,300) for each day the offense continues after conviction.

The MHA and the SPF are also offering Meta assistance to identify other influential public figures in Singapore who may be at risk of being impersonated by scammers.

Increase in Social Media Scam Schemes

Singapore's MHA observed an increase in scam campaigns on social media between June 2024 and June 2025, including fake advertisements with profiles and pages impersonating government staff members.

Facebook was the top platform where these scams appeared over the reported period, according to the MHA.

Between June 2024 and June 2025, SPF disrupted approximately 2000 such scam advertisement schemes on Meta's platform.

"Stemming the proliferation of such impersonation scams is critical to protect the public from harm

and uphold trust in our government and public institutions," the ministry said in a statement.

While the MHA has acknowledged that Meta has already taken steps to address the risk of impersonation scams, these were not deemed sufficient to curb the prevalence of such scams in Singapore.

Big Tech Must Do More Against Online Scams, Expert Argues

JonathanFrost, director of global advisory for EMEA at BioCatch and former leader of the UK's National Fraud and Cybercrime Reporting system at the City of London Police,welcomed the decision. However, he said he feared it is not enough to prompt Meta to step up its fight against online scams.

"Singapore's crackdown on Meta is a step in the right direction, but the relatively small fine is not enough of a deterrent to demand real accountability from Big Tech. The SPF's disruption of 2000 fraud ads on Facebook is just a drop in the ocean, and the issue must be tackled by regulators on a global scale," he explained.

He argued that Big Tech should follow the blueprint of the financial sector and invest much more into anti-scamming measures.

"Banks invest billions in tech to safeguard consumers, and shoulder the responsibility for stopping scams, yet fraud typically begins further upstream, on websites and social media. Meanwhile, Big Tech firms profit billions from fraud ads, with 70% of new Facebook and Instagram advertisers being scammers. Only a coordinated global regulatory response will hold Big Tech to account, compel intelligence-sharing and protect consumers from losing life changing sums of money," he said.

The Singapore government added that it was considering issuing similar requirements to other social media platforms.