GSMA

Case Study: Maxis

Scam prevention - blocking through a multi-layered national framework

Case Study: Maxis

Scam prevention blocking through a multi-layered national framework

Asia Pacific | SMS Phishing (Smishing) Detection | Maxis

Scam blocking across Malaysia requires coordination between operators, regulators, and law enforcement.

Maxis built a multi-layered framework that combines regulatory compliance with internal detection and field operations. The framework targets three distinct threat vectors: fraudulent messages and calls, malicious websites, and rogue base stations. Together, those layers make scam execution significantly harder.

Maxis collaborates with the Malaysian Communications and Multimedia Commission (MCMC) and other national agencies through the National Scam Response Centre. That partnership links Maxis's technical controls to real enforcement outcomes on the ground.

Solution

Scam SMS and calls blocking through firewalls, and gateway controls

The Malaysian Communications and Multimedia Commission (MCMC) directed operators to block SMS containing URLs, requests for customer information, and callback numbers. Maxis implemented SMS firewall controls that also block messages matching specific keywords, phrases, and text patterns. In addition, Maxis runs a Fraud Management System (FMS) that detects abnormal sending behaviour and unusual traffic volumes. When the FMS flags a pattern as suspicious, it blocks matching messages automatically.
Maxis scam call blocking also extends to its International Gateway. Those rules stop messages claiming to originate from Malaysian mobile and fixed numbers that arrive via international routes. They also block calls carrying non-existent country codes. Maxis participates in the Inter-Operator CLI Spoofing arrangement that allows each operator to check Malaysian mobile numbers coming through International Gateway to ensure only legitimate roaming customer calls are allowed to pass through.

Website blocking at network level

Maxis implements the website blocking based on the government's instructions to block access to harmful and illegal websites, including phishing domains within the timeline required by the regulator.

Fake BTS tracing and national law enforcement collaboration

Fake base transceiver stations can inject scam SMS directly into a mobile handset, bypassing standard operator controls. Maxis developed an award winning Fake BTS Detection Dashboard. The platform detects threats and patterns, and provides critical information for ground surveillance to use to identify Fake BTS deployments. When the team identifies suspicious activity, it escalates the details to its internal Fraud Prevention and Cybersecurity units, MCMC, and the Royal Malaysia Police. The Royal Malaysia Police have carried out multiple successful enforcement actions as a result of those escalations.

Maxis also collaborates with the National Anti-Financial Crime Centre and the Royal Malaysia Police through the National Scam Response Centre, reachable on 997. That three-way collaboration connects Maxis's technical detection capability to formal investigation and prosecution channels. Furthermore, Maxis warns customers through SMS alerts, social media, website notices, and in-app messages. An inter-operator anti-spoofing solution is also under development to validate caller numbers across Malaysia's mobile networks. That solution will provide additional protection by preventing cross-network number spoofing.

Impact

Scam blocking outcomes across Malaysia

Following the MCMC directive, Maxis's scam SMS blocking measures contributed to a 65% drop in scam SMS deliveries. That reduction occurred between Q4 2024 and Q1 2025, over the course of a single quarter. The Fraud Management System and SMS firewall also filtered out additional messages through keyword detection and behavioural thresholds.

Maxis's Fake BTS tracing work led to multiple successful law enforcement actions by the Royal Malaysia Police. Those enforcements removed rogue hardware that standard filters cannot reach. However, scammers continue to adapt by shifting to OTT platforms such as WhatsApp and Facebook, which fall outside direct operator control. Overall, Maxis's layered approach has made scam delivery more difficult and demonstrated the value of combining technical controls with field surveillance.

Additional information	
Participating organisations:	maxis, MCMC, Royal Malaysia Police
Location:	Asia Pacific, Malaysia.