GSMA

Case Study: Dialog Axiata

Scam SMS protection through real-time URL screening and visual security warnings

Case Study: Dialog Axiata

Scam SMS protection through real-time URL screening and visual security warnings

Asia Pacific | Scam SMS Protection | Dialog Axiata

As Sri Lanka's largest mobile operator — with around **70% subscriber market share** across its two brands, Dialog and Airtel — Dialog Axiata operates on a national scale and carries a corresponding responsibility to act to prevent scams: it chose to move first and lead by example rather than wait for the wider industry to follow. A survey conducted by Dialog found that **20% of users** had been targeted by scammers over the past two years, of whom **around half** ended up falling victim, and **30% of victims** lost more than a month's income to scams. These findings compelled Dialog to take immediate action. Protecting subscribers from scam SMS at scale means catching a malicious link before the customer taps it, not after they report a loss. Dialog handles around 30 million SMS messages in a typical day, of which **1.2 million messages** carry an embedded URL — a channel that scam and phishing operators exploit to reach customers directly.

Scammers abuse both application-to-person (A2P) and person-to-person (P2P) messaging to spread these links; A2P carries the bulk of the malicious volume, while the P2P channel is exploited at a much lower share **(less than 1% of the total malicious URLs uses P2P channel)**. Because campaigns rotate domains rapidly and a subscriber cannot reliably tell a legitimate link from a malicious one, controls that act only after complaints arrive always come too late.

Dialog needed scam SMS protection that screened links in real time, at the point of delivery. In **June 2026**, Dialog deployed a network-level SMS URL screening capability that inspects links as messages transit the network and attaches a clear visual security warning to any message found to carry a scam link — alerting the subscriber before any interaction takes place.

Solution

Real-time scam detection on URL-bearing SMS

Dialog screens every URL-bearing SMS as it passes through the network. Each link is evaluated in real time against multi-source threat intelligence and classified by risk. Because the assessment happens in transit rather than in response to a customer complaint, a scam link is identified at the moment it would otherwise reach the subscriber — before any interaction takes place.

Alerting subscribers with a visual security warning

The screening outcome drives a graduated response. High confidence, dangerous links are blocked outright so the message is never delivered. For the broader tier of suspicious links — where an outright block would risk withholding a legitimate message — the SMS is still delivered, but Dialog attaches a clear visual security warning (**Dialog Warning SPAM** or **Airtel Warning SPAM** depending on which network the recipient belongs to) to the message itself before it reaches the customer.

The subscriber sees an explicit alert identifying the link as a potential scam, at the exact point of exposure, and can decide accordingly. The message is still delivered, so genuine communication is never disrupted — but the customer is no longer left to judge an unfamiliar link unaided.

This approach gives subscribers an informed choice without disrupting legitimate messaging, while every flagged message and its treatment is logged for continuous monitoring and reporting. In turn, that visibility supports ongoing tuning of detection thresholds and campaign-level investigation.

Reporting malicious senders and cross-industry collaboration

Detection also builds an evidence base of the sender identities behind scam campaigns. As a starting measure, Dialog is reporting these identified malicious senders to the Telecommunications Regulatory Commission of Sri Lanka (TRCSL) for regulatory awareness and action. Recognizing that scam operators move fluidly between networks, Dialog further intends to work closely with other mobile network operators to share the identified malicious senders with one another — so that a sender exposed on one network can be recognized and acted upon across the industry, and subscriber protection does not depend on which network a message happens to traverse.

Impact

Scam SMS protection outcomes

In the first 33 days after launch, Dialog screened **close to 40 million** URL-bearing messages and identified approximately **6 million** messages with suspicious URLs - **14.9**% of all URL-bearing traffic - spanning 5,900 + distinct malicious domains. Of these, **3.1 million** were blocked before delivery and **2.9 million** were delivered carrying a visual security warning, giving subscribers an explicit alert at the moment of exposure.

These figures confirm that screening links in real time is more effective than reacting to complaints after a scam has already reached the customer, and that a visual security warning protects subscribers without disrupting legitimate messaging. A residual **200,000+** scam messages still reached subscribers on networks outside Dialog's scope — which is why Dialog is escalating malicious senders to the TRCSL and pursuing sender-sharing with other operators, so that protection becomes consistent across the industry rather than depending on which network a subscriber is on.

Additional information	
Participating organisations:	Dialog
Location:	Asia Pacific, Sri Lanka.