Lookout

Mobile Threat of the Month

February 2026

SMS Blaster Fraud on the London Underground

Security experts and law enforcement have identified a rise in "SMS Blaster" scams targeting mobile users. A recent case involves targeting London Underground passengers using portable devices concealed in suitcases.

What is SMS Blasting?

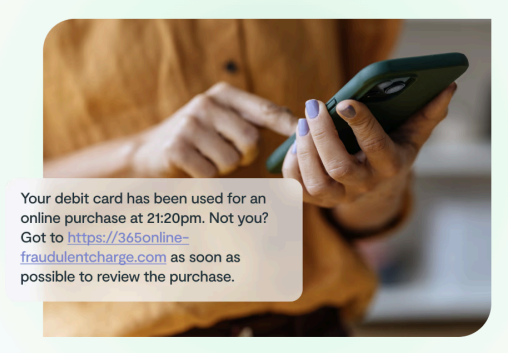
SMS blasting involves portable surveillance devices that mimic cell towers to hijack phone connections and send mass "smishing" (SMS phishing) texts, often impersonating trusted entities like Evri or Royal Mail to steal sensitive data. To bypass encryption, the device often forces connected phones to downgrade from 4G/5G to the less secure 2G protocol, rendering carrier spam filters useless. These devices can affect phones within a radius of up to 1,000 meters (3,280 feet) and can send as many as 100,000 text messages per hour.

The London Underground Plot

A gang reportedly travelled through the London Underground with heavy suitcases containing homemade SMS blasters. The Tube was chosen as a "hunting ground" due to its crowded environment and limited legitimate signal, making phones more likely to latch onto the fake signal. Passengers in the vicinity received fake texts claiming to be from delivery services like Evri or Royal Mail, warning of "failed deliveries" and urging them to click a link to reschedule. These links led to fraudulent websites designed to steal sensitive information such as banking details and login credentials. The plot unravelled when a British Transport Police officer became suspicious after spotting a large suitcase being dragged around covered in ventilation holes.

Lookout Mobile Security

Because SMS blasters impersonate legitimate cell towers to trick nearby devices, standard carrier-level protections are often ineffective. Security must instead be managed directly on the endpoint. Lookout provides dedicated mobile defence layers that detect these rogue base stations, preventing SMS blaster attacks from leading to full-scale business compromise.



Mobile Phishing Protection: Detects and blocks mobile phishing attacks across any messaging app that directs users to malicious URLs or phishing websites.

Smishing Protection: Industry first AI driven SMS phishing detection that identifies attempts to manipulate employees into revealing sensitive data.

Mobile Network Security: Lookout analyses new network connections in real time to detect and block connectivity to unsafe cellular or WiFi networks.

Lookout helps organisations secure the rapidly growing mobile workforce environments by closing visibility gaps that traditional security tools don't cover.

Sources: TechRadar, The Standard