ZIMPERIUM

Zimperium Advanced AI Smishing Analysis

AI-empowered SMS Phishing Defense to stop AI driven attacks

Executive Summary

Cybercriminals have moved to a mobile-first attack strategy and social engineering is their preferred strike vector. Mishing (mobile-targeted phishing) tactics have evolved with easy access to AI that is being leveraged to increase the speed, scale and sophistication of attacks, including the use of conversational scams, brand and executive impersonation, and QR codes and fraudulent images delivered via text and encrypted messaging applications that bypass traditional security controls.

Zimperium's Advanced AI Smishing Analysis is a premium feature that leverages the most sophisticated frontier AI models to identify and protect against malicious text and images from both native mobile messaging functions (Apple iMessage and Android's Google Messages) and third-party encrypted messaging apps (WhatsApp, Telegram, Signal, and others).

The Evolving Threat Landscape: The Rise of Linkless & Image-Based Mishing

Traditional defense solutions that are dependent on URL reputation databases to block phishing attempts are ineffective against today's AI driven Smishing attacks, which intentionally avoid the use of links. Supported by widely available AI tools, attackers have shifted to well crafted plain text messaging, as well as embedded images, such as QR codes, which easily bypass traditional methods of detection and appear harmless to even the most diligent employees:

Messaging App and Conversational Scams
Attackers leverage native device SMS and popular third-party messaging applications (e.g., WhatsApp, Telegram and others) to build trust or create artificial urgency.

Executive Impersonation
Posing as corporate leadership or trusted business partners to manipulate employees into transferring funds, or sharing private data.

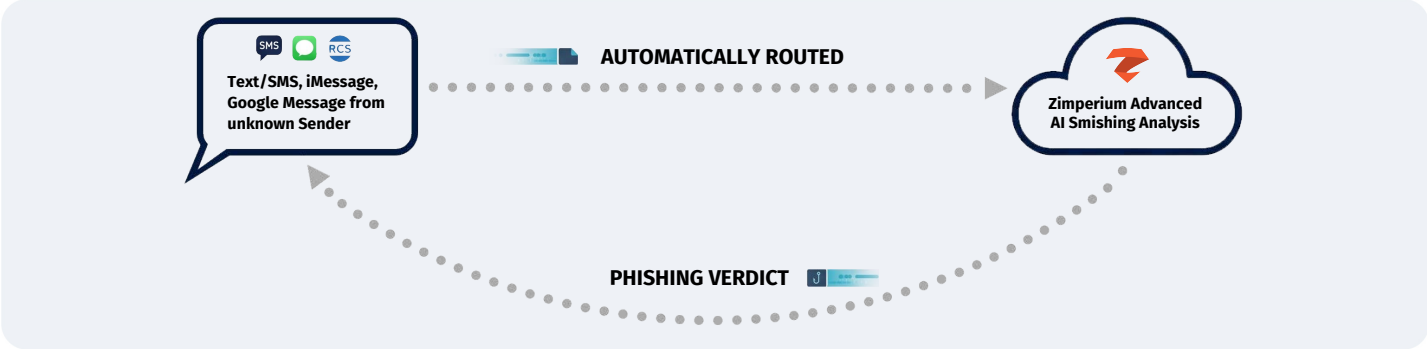
Image-Based Phishing (QR Codes & Visual Scams)
QR codes that link to fraudulent login pages (Quishing), text commands embedded within images, and impersonated logos of trusted brands slip past enterprise perimeters unnoticed, while deceiving users to gain further access to corporate credentials and networks.

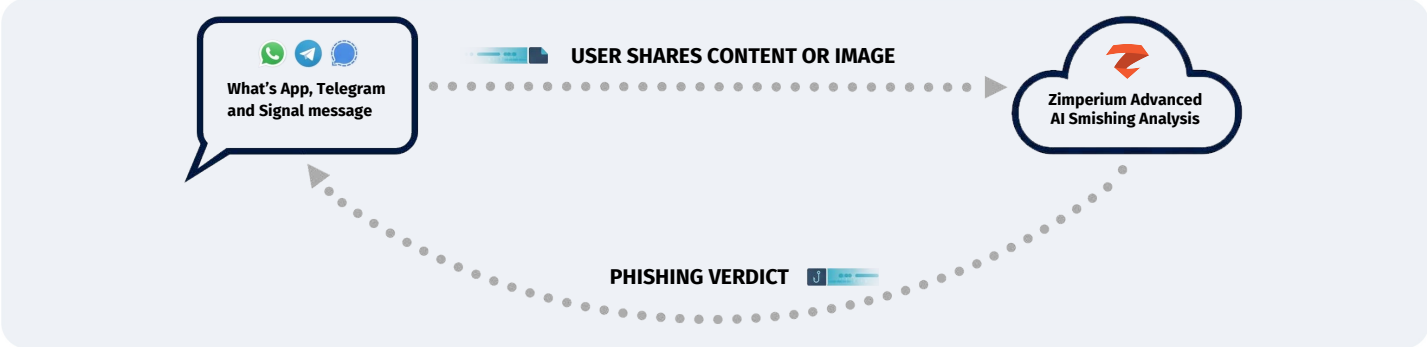
The Solution: Automated AI-empowered Phishing analysis of SMS and Messaging from Unknown Senders

Zimperium offers Advanced AI Smishing Analysis as a premium add-on feature available to all MTD customers. Utilizing the latest of cloud-based AI models, SMS/text messages, images and QR codes are analyzed to identify malicious intent, stopping threats and protecting users from even the most sophisticated social engineering attacks.

Advanced AI Smishing Analysis **autonomously** inspects all messages sent via native mobile messaging functions (Apple iMessage and Android's Google Messages) from unknown senders without requiring manual intervention from the user, identifying malicious content automatically.

Smishing attacks targeting encrypted third-party messaging apps have skyrocketed in both scale and effectiveness. With Advanced AI Smishing Analysis users of WhatsApp, Telegram, Signal, and other encrypted messaging apps are protected against malicious content by simply submitting suspicious messages and images for AI analysis via the MTD app.





Key Benefits of Advanced AI Smishing Analysis

- **Zero-Link & Conversational Intent Detection:** extends phishing protection to linkless messages leveraging conversational social engineering techniques to initiate an attack. Advanced AI models analyze message text content for indications of phishing, stopping scams before they progress to credential collection, corporate network penetration, or financial fraud.
- **Image Analysis:** Advanced AI models extract text from images and analyze for indicators of phishing and fraudulent structures, identifying spoofed logos, credential-harvesting layouts, and indicators of executive impersonation.
- **True Multi-Channel Protection:** Extends protection across the entire mobile communication surface. Protection is applied to SMS/Text, native OS messaging applications as well as encrypted third-party platforms like WhatsApp, Telegram and Signal.

About Zimperium

Zimperium is the world leader in AI-empowered mobile security. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging the power of AI to deliver autonomous security that counters evolving threats including mishing, malware, and zero-day attacks.

To learn more about securing your mobile fleet against advanced AI powered messaging threats, visit www.zimperium.com.

ZIMPERIUM®

Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244

© 2026 Zimperium, Inc. All rights reserved.