iVerify Expands Mobile EDR with SmishGuard to Stop Mobile Phishing and Identity Compromise

SmishGuard addresses a high-converting initial access vector in enterprise security: mobile messaging attacks that bypass email and endpoint controls.

iVerify logo

BELFAST, NORTHERN IRELAND & NEW YORK, NY, UNITED STATES, May 6, 2026 /EINPresswire.com/ -- iVerify, the leader in advanced mobile endpoint detection and response (EDR) solutions, today announced the launch of SmishGuard, a mobile-native defense against SMS and voice-based social engineering. SmishGuard addresses one of the highest-converting initial access vectors in enterprise security: mobile messaging attacks that bypass traditional email and endpoint controls.

Mobile devices have become the primary identity and access layer for enterprise users through phone-based multi-factor authentication, but remain largely unprotected against sophisticated social engineering attacks. Smishing, or SMS/RCS phishing, is now the number one delivery vector for credential theft on mobile. Users are six to ten times more likely to click SMS phishing links compared to email, and 80% of phishing sites are optimized for mobile. When combined with a SIM swap, smishing creates a direct path for 2FA bypass and account takeover.

Traditional defenses are proving ineffective as messaging moved from SMS to encrypted RCS, rendering carrier filtering, secure SMS gateways, and mobile threat defense (MTD) solutions ineffective. Legacy solutions are reactive, blind to encrypted RCS, and fail against linkless spear phishing and voice-based attacks, known as vishing. Traditional phishing filters operate on known-bad URL lists, meaning any malicious domain not already observed and cataloged will pass through unblocked. Attackers exploit this predictably, rotating infrastructure to stay ahead of blocklists. A growing share of mobile social engineering attacks sidestep the problem entirely, carrying no URL at all and relying on message content alone to manipulate recipients into disclosing credentials or authorizing transactions.

SmishGuard is the first enterprise-grade smishing protection solution designed to detect linkless

attacks and work across messaging platforms, including SMS, RCS, WhatsApp, and Signal. Its core differentiation lies in its privacy-preserving architecture. Only the information required to determine whether a message is malicious is analyzed, and no unnecessary user data is ever retained. SmishGuard is multi-layered, combining cloud-based analysis with fleet-wide threat intelligence to protect users without compromising privacy, a critical factor for BYOD adoption:
-- Multifactorial Cloud-Based Analysis: Messages from unknown senders are analyzed through a privacy-preserving cloud pipeline that evaluates sender reputation, message content, and behavioral signals to determine whether a message is malicious.
-- Advanced Detection: The platform uses natural language processing to analyze content for manipulation patterns like urgency, authority, and fear, alongside an ML model for spear-phishing signals instead of relying on known bad URL matching.
-- Cross-Platform Coverage: It ingests messages via SMS and uses OCR-based ingestion for content shared via screenshots on WhatsApp, Signal, and iMessage.
-- Fleet-Wide Protection: Confirmed threats propagate across devices through fleet-wide intelligence, enabling real-time blocking of malicious numbers, domains, and VoIP sources for the entire organization.
-- Integration: Alerts stream directly into SIEM/XDR platforms, providing SOC teams with visibility into mobile attacks and integration into existing workflows.

"Mobile attacks have evolved far past what existing MTD and email security tools were built to handle, turning mobile devices into a credential faucet," said Rocky Cole, COO and co-founder of iVerify. "Phones now hold the keys to enterprise identity through MFA and SSO, yet SOC teams have had no visibility into what's happening in SMS, WhatsApp, or voice channels. SmishGuard closes that gap, giving security teams the signal they need to stop social engineering before it becomes an identity compromise and reinforcing Zero Trust at a layer that has been largely unmonitored."

The launch of SmishGuard expands iVerify's platform from device security to identity protection, and adds social engineering defense to its mobile EDR product at no additional cost.

To learn more about SmishGuard, register for our webinar, or to book a demo, visit www.iverify.com.

About iVerify
iVerify is a pioneer in mobile endpoint detection and response (EDR) solutions, providing advanced protection against the real threats mobile devices face. The company's comprehensive security platform safeguards organizations from fileless malware, smishing, malicious applications, ransomware operations, and breaches resulting from credential theft. iVerify's solutions span from consumer to enterprise and government sectors, offering both privacy-focused BYOD protection and enterprise-grade security capabilities to ensure every device in the workplace is secure.

For more information, please visit: www.iverify.com.

Monika Hathaway
iVerify
email us here
Visit us on social media:
LinkedIn
X
