SmishGuard: Mobile-Native Defense That Stops Smishing Attacks at Source

iVerify.

Detect and block smishing, vishing, and link and linkless attacks that bypass traditional mobile security controls.

Smishing has become the leading vector for credential theft on mobile, with users up to 10x more likely to click malicious message links than email. Yet traditional defenses are ineffective against modern mobile social engineering due to critical blind spots:

Blind to Encrypted Messaging: Carrier filtering is circumvented by end-to-end encrypted protocols like RCS.

Failure Against Linkless Attacks: Traditional tools are often reactive and IOC-based, failing against linkless spear phishing and vishing attacks.

Misaligned Focus: Mobile Threat Defense (MTD) vendors primarily focus on malware and device posture, lacking robust social engineering detection.

Security Gaps: Email security solutions do not cover critical mobile messaging ecosystems like SMS, WhatsApp, and Signal.

Mobile devices are the front door to enterprise access, and this visibility gap creates a critical initial access path for attackers that often leads to broader enterprise compromise.

Introducing SmishGuard by iVerify

SmishGuard is a mobile-native social engineering defense platform designed to protect every employee across the enterprise. It detects and blocks multi-channel threats across the mobile ecosystem:

- **Smishing** (SMS/RCS phishing)
- **Vishing** (voice-based attacks)
- **Linkless spear phishing** (no URL required to compromise a target)
- **Cross-platform attacks** across SMS, RCS, WhatsApp, and Signal

Mobile Protection Without User Friction

- **Reduce Account Takeover Risk:** Dramatically lower the risk of account takeover by blocking the #1 delivery vector for credential theft on mobile devices.
- **Enable Secure BYOD Adoption:** Deploy enterprise-grade protection across employee-owned devices without requiring invasive tooling or compromising user privacy.

SmishGuard Deployment

SmishGuard deploys as a mobile-native extension of the iVerify Mobile EDR platform. Protection is active from installation, no complex configuration required. Security teams configure alert streaming directly into their existing SIEM/XDR infrastructure.

- **Expand SOC Visibility:** Gain critical visibility into the mobile attack surface by integrating alerts directly into existing SIEM/XDR workflows.
- **Protect Every Employee:** Defend the entire workforce, including executives and employees with sensitive system access, from targeted spear phishing and voice impersonation attacks.

Where SmishGuard Delivers the Most Value

Securing Every Employee

Every employee with a mobile device is a potential target. SmishGuard provides comprehensive defense across the entire workforce, on both BYOD and managed devices, without friction or invasive controls.

Protecting High-Risk Users

Executives and other high-value targets face disproportionate risk from targeted spear phishing and multi-channel social engineering attacks. SmishGuard's behavioral detection is built to catch the sophisticated, linkless attacks most commonly directed at them.

Closing the Identity Access Gap

Mobile-delivered credential harvesting and sideloading attempts are increasingly used as the initial access point for broader enterprise compromise. SmishGuard neutralizes that path before attackers can establish a foothold.

Privacy Features

Designed for secure BYOD adoption, SmishGuard is built with a privacy-first architecture. Messages from unknown senders are analyzed through a privacy-preserving cloud pipeline that cannot identify the originating device or recipient. Messages confirmed as safe are never retained. Only a structured finding indicating whether a message is malicious is ever shared with authorized SOC personnel.

Stop Mobile Social Engineering Before Identity Compromise.

Book a Demo to see how SmishGuard closes the identity access gap in your organization and protects your high-value assets.