CISOs Face Widening Gaps in Defending Multi-Channel Social Engineering Threats

Dune Security's new study reveals enterprises rarely simulate attacks from APT groups like Scattered Spider, despite 64% facing multi-channel breaches in the past year.

New York City, New York Sep 4, 2025 (Issuewire.com) - As social engineering attacks evolve to exploit encrypted messaging, SMS, collaboration tools, and voice calls, enterprises remain stuck preparing users only for email threats, according to new data from Dune Security. This mismatch leaves organizations vulnerable, even as high-profile breaches highlight the risks.

Drawing from Dune Security's 2025 Insider Threat Intelligence Report, including survey data from leading enterprise CISOs (Chief Information Security Officers) and behavioral telemetry from its simulation engines, concern outpaces action across vectors. For instance, 71% of CISOs worry about SMS phishing (smishing), yet only 27% simulate it; 59% fear voice phishing (vishing), but just 15% test it. Testing for collaboration tools and encrypted messaging? It plummets to single digits or zero, despite 38% concern for attacks coming from these channels.

Key findings include:

- Only 12% of CISOs believe their current Security Awareness Training (SAT) program is sufficient.
- 0% of surveyed enterprises simulate threats in encrypted messaging apps, even as 64% confirmed social engineering attacks via encrypted or informal channels in the past 12 months.
- Just 18% of organizations tailor phishing simulations by both role and behavior, though 91% say this is essential.
- While 100% test email phishing, only 15% simulate vishing and 27% test smishing.
- AI-personalized phishing now drives 300% more user interaction than traditional, templated variants.

"Attackers are exploiting the blind spots where enterprises aren't defending," said David DellaPelle, CEO and Co-Founder of Dune Security. "Legacy SAT programs are limited to yesterday's email threats while real breaches now start in high-trust, low-visibility channels like encrypted messaging, SMS, voice call, and deepfake-based impersonation."

Forward-thinking security teams are now shifting away from checkbox training toward behavior-based simulation, real-time visibility, and adaptive remediation. Dune's latest data confirms that legacy

awareness programs fail not due to lack of effort, but because the embedded technology misses where risk actually lives: in untested channels and unmonitored user behavior.

“Traditional solutions simply can’t keep up with today’s evolving threats or the way people actually work,” said Dune Security Senior Manager of Engineering and AI, Kyle Ryan.

“Our platform proactively red-teams our customers’ organizations, using the same social engineering attack modalities that hackers are deploying in the wild. We hyper personalize testing, training, and control guardrails to each employee’s role, level, industry, strengths, and weaknesses, empowering them to protect both themselves and their organizations in real time."

The 2025 Insider Threat Intelligence Report draws on survey responses from industry-leading enterprise CISOs, combined with proprietary simulation and behavioral analytics from Dune Security’s platform. The report details attack channel trends, readiness gaps, and the behavioral triggers most likely to lead to compromise.

About Dune Security

Dune Security helps enterprises quantify and reduce user cyber risk. Dune’s User Adaptive Risk Management solution automatically prevents insider threat and social engineering by simulating multi-channel attacks, scoring user risk, and adapting remediation in real time. Dune is trusted by Fortune 1,000s including Hugo Boss, Warner Music Group, and Culligan.

Learn more at dune.security.

Media Contact

Grace Gately

*********@dune.security

Source : Dune Security

See on IssueWire