B2B SAAS PLATFORM

LudiSec

WHITEPAPER

The State of Phishing in 2026

Document Information

Published	June 10, 2026
Uploaded	2026-06-10
Author	Joan Fontbona
Classification	Public

Executive Summary

EXECUTIVE SUMMARY

Phishing remains the primary entry vector for enterprise cyber breaches. In 2026, the landscape shifted significantly due to the commoditization of generative AI models, which allow malicious actors to automate hyper-personalized spear-phishing campaigns at scale. This report analyzes data from over 10,000 organizational security incidents to outline tactical defense strategies.

KEY FINDINGS AND EVOLVING THREATS

First, 68% of documented enterprise breaches originated directly from a phishing email. Second, AI-crafted lures bypass legacy signature-based spam filters at a 42% higher rate because they lack grammatical errors and adapt tone dynamically to mimic corporate vendors. Third, the average time to detect a credential compromise via phishing sits at 197 days, giving attackers ample lateral movement windows. Fourth, we have observed a sharp increase in Quishing (QR code phishing) which shifts the attack vector to unmanaged mobile devices, bypassing corporate network inspection.

THE ADVANCED PREVENTION FRAMEWORK

To combat these modern threats, a multi-layered defensive posture is mandatory:

Layer 1: Continuous Awareness Training. Implement gamified simulations every 90 days. Short, interactive training experiences yield a 76% behavioral improvement over annual compliance lectures.

Layer 2: Hardened Authentication. Enforce hardware-based FIDO2 multi-factor authentication. Discontinue SMS and voice-based MFA which are highly vulnerable to real-time proxy interception tools like Evilginx.

Layer 3: Protocol Optimization. Deploy strict email authentication policies including DMARC set to reject, along with robust SPF and DKIM record verification across all corporate subdomains.

OPERATIONAL CONCLUSION

Relying on technology filters alone creates a dangerous false sense of security. Organizations must build a resilient security culture where employees serve as a proactive detection layer. Integrating real-time reporting utilities ensures rapid containment before an initial intrusion escalates into a catastrophic enterprise ransomware incident.

1. Introduction

> *This report explores the evolving landscape of phishing attacks in 2026, focusing primarily on AI-driven threats and evasion techniques.*

2. Background & Context

Generative AI has lowered the barrier to entry for cybercriminals, resulting in highly convincing, grammatically perfect, and localized spear-phishing campaigns at scale.

3. Methodology

Analysis based on telemetry data and post-mortem reviews from over 10,000 reported enterprise phishing incidents globally over a 12-month period.

4. Findings

AI-crafted lures bypass traditional spam filters at a 42% higher rate, while the average time to detect a compromise remains alarmingly high at 197 days.

5. Recommendations

Adopt FIDO2 hardware keys for MFA, implement strict DMARC/SPF/DKIM policies, and deploy continuous gamified security awareness training.

6. Conclusion

Organizations must shift from periodic compliance-based training to continuous behavioral modification to effectively counter modern phishing techniques.

7. References

1. 2026 Global Threat Intelligence Report. 2. Anti-Phishing Working Group (APWG) Annual Trends.

About LudiSec

LudiSec is a cybersecurity risk management platform headquartered in Barcelona, Spain. Serving enterprise clients across financial services, healthcare, manufacturing, and the public sector. Available in English, Spanish, and Catalan.