PLATAFORMA SAAS B2B

LudiSec

WHITEPAPER

L'Estat del Phishing al 2026

Informació del document

Publicat	June 10, 2026
Pujat	2026-06-10
Autor	Joan Fontbona
Classificació	Publica

Resum Executiu

RESUM EXECUTIU

El phishing continua sent el principal vector d'entrada per a les ciberbretxes empresarials. El 2026, el panorama va canviar significativament a causa de la democratització dels models d'IA generativa, fet que permet als actors maliciosos automatitzar campanyes de spear-phishing hiperpersonalitzades a gran escala. Aquest informe analitza dades de més de 10.000 incidents de seguretat organitzacional per traçar estratègies de defensa tàctica.

TROBALLES CLAU I AMENACES EN EVOLUCIÓ

Primer, el 68% de les bretxes empresarials documentades es van originar directament en un correu electrònic de phishing. Segon, els senyuels creats per IA evadeixen els filtres de correu brossa tradicionals basats en signatures amb una taxa un 42% més alta perquè no tenen errors gramaticals i adapten el to dinàmicament per imitar els proveïdors corporatius. Tercer, el temps mitjà per detectar un compromís de credencials a través de phishing és de 197 dies, cosa que ofereix als atacants àmplies finestres de moviment lateral. Quart, hem observat un marcat augment en el Quishing (phishing amb codis QR) que desplaça el vector d'atac a dispositius mòbils no gestionats, evitant la inspecció de la xarxa corporativa.

MARC DE PREVENCIÓ AVANÇAT

Per combatre aquestes amenaces modernes, és obligatori adoptar una postura defensiva de múltiples capes:

Capa 1: Formació contínua en conscienciació. Implementar simulacions gamificades cada 90 dies. Les experiències de formació curtes i interactives generen una millora del comportament del 76% en comparació amb les conferències de compliment anuals.

Capa 2: Autenticació robusta. Fer complir l'autenticació multifactor FIDO2 basada en maquinari. Descontinuar MFA basat en SMS i veu, que són altament vulnerables a les eines d'intercepció pròxi en temps real com Evilginx.

Capa 3: Optimització de protocols. Desplegar polítiques estrictes d'autenticació de correu electrònic, incloent DMARC configurat en rebutjar, juntament amb una verificació sòlida de registres SPF i DKIM en tots els subdominis corporatius.

CONCLUSIÓ OPERATIVA

Confiar únicament en els filtres tecnològics crea una perillosa falsa sensació de seguretat. Les organitzacions han de construir una cultura de seguretat resilient on els empleats actuin com una capa de detecció proactiva. La integració d'utilitats d'informes en temps real garanteix una contenció ràpida abans que una intrusió inicial es converteixi en un incident de ransomware empresarial catastròfic.

1. Introducció

> *Aquest informe explora el panorama evolutiu dels atacs de phishing el 2026, centrant-se principalment en les amenaces impulsades per IA i les tècniques d'evasió.*

2. Marc i context

> *La IA generativa ha reduït la barrera d'entrada per als ciberdelinqüents, donant lloc a campanyes de spear-phishing altament convincents, gramaticalment perfectes i localitzades a gran escala.*

3. Metodologia

> *Anàlisi basada en dades de telemetria i revisions post-mortem de més de 10.000 incidents de phishing empresarial reportats globalment durant un període de 12 mesos.*

4. Troballes

> *Els senyuels creats per IA evadeixen els filtres de correu brossa tradicionals amb una taxa un 42% més alta, mentre que el temps mitjà per detectar un compromís continua sent alarmantment alt: 197 dies.*

5. Recomanacions

> *Adoptar claus de maquinari FIDO2 per MFA, implementar polítiques estrictes de DMARC/SPF/DKIM i desplegar formació gamificada contínua de conscienciació en seguretat.*

6. Conclusions

> *Les organitzacions han de passar d'una formació periòdica basada en el compliment a una modificació contínua del comportament per contrarestar eficaçment les tècniques modernes de phishing.*

7. Referències

1. Informe Global d'Intel·ligència d'Amenaces 2026. 2. Tendències anuals de l'Anti-Phishing Working Group (APWG).

Sobre LudiSec

LudiSec és una plataforma de gestió de riscos de ciberseguretat amb seu a Barcelona, Espanya. Serveix a clients empresarials de serveis financers, sanitat, indústria manufacturera i el sector públic. Disponible en anglès, castellà i català.