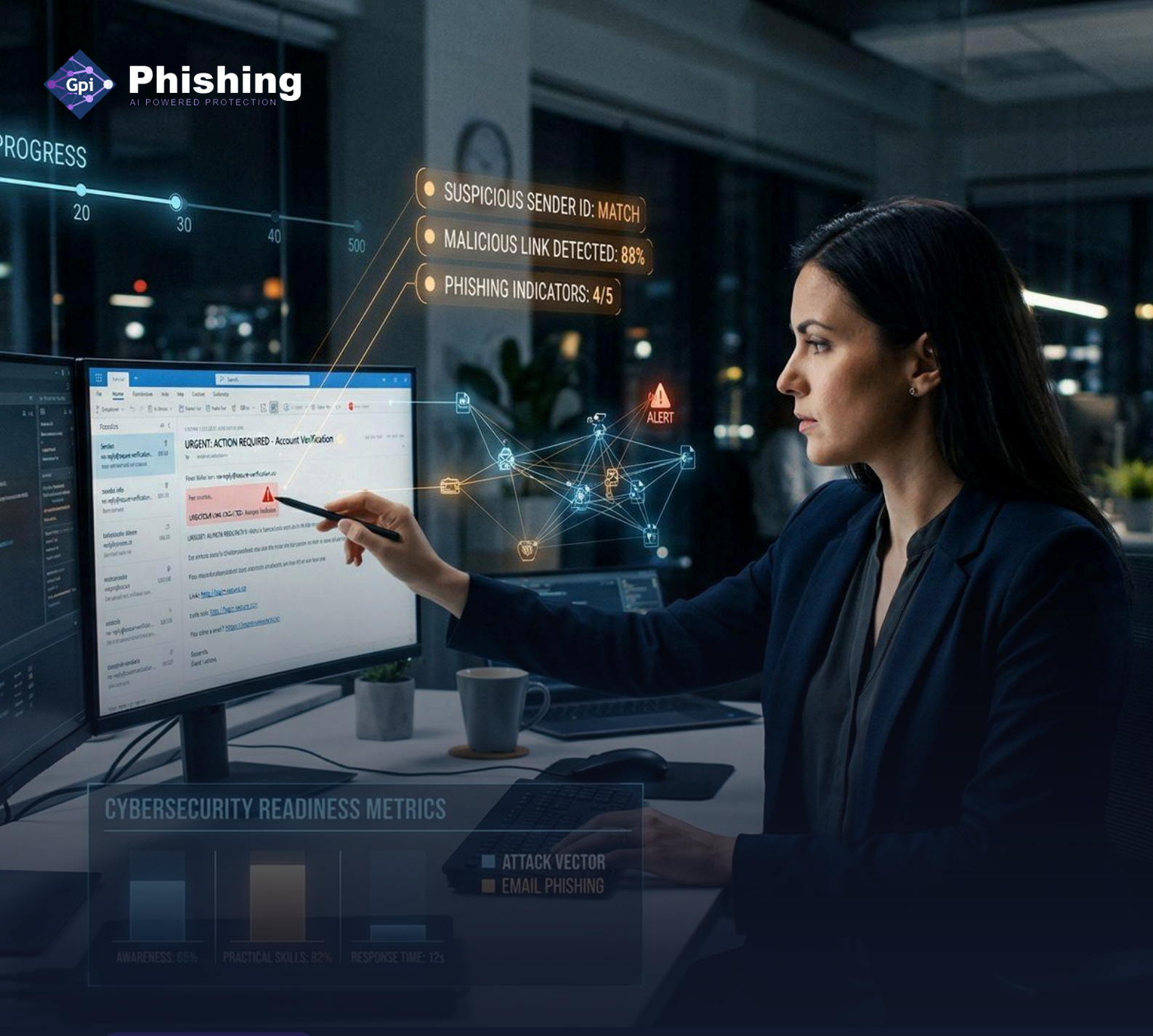

THREAT AWARENESS

Simulazioni di Phishing: perché la formazione senza pratica non basta

Test, feedback, misurazione psicometrica: il modello a “sandwich” per costruire resilienza reale

A cura del team CENANT di GPI Cyberdefence

01 aprile 2026 www.gpiphishing.com

THREAT AWARENESS

Test, feedback, misurazione psicometrica: il modello a “sandwich” per costruire resilienza reale

01 Sapere non è saper fare

Un dipendente che ha letto una guida sul phishing sa come dovrebbe comportarsi. Ma la stessa persona, nel mezzo di una giornata lavorativa intensa, con venti e-mail da smaltire e una riunione tra dieci minuti, può cliccare su un link malevolo ben costruito senza neppure accorgersene. La conoscenza teorica, da sola, non crea i riflessi giusti.

È per questo che le simulazioni di phishing, e-mail-trappola inviate ai dipendenti in condizioni reali, sono diventate uno strumento fondamentale nei programmi di security awareness più efficaci.

02 I dati che convincono i board

Le aziende che implementano programmi di phishing simulation costante, combinati con formazione interattiva e una cultura della segnalazione, riducono il tasso di click sulle e-mail-trappola da un range iniziale del 20-30% a valori del 4-5% o inferiori nel corso di dodici mesi.[2]

Google ha implementato un sistema di formazione obbligatoria con simulazioni regolari di phishing per i propri dipendenti: dopo sei mesi, il tasso di successo degli attacchi simulati si è ridotto dal 28% al 4%.[4] Non è un'eccezione, è un risultato replicabile con un programma strutturato.

RIFERIMENTI

1 Proofpoint Human Factor Report (2022).
2 GPI Cyberdefence, analisi multicaso (2025).
3 FBI Internet Crime Report (2023).
4 Google Security Blog.

03 Il modello a 'sandwich'

I programmi di awareness più efficaci seguono una struttura ciclica che alterna valutazione, pratica e formazione. **Prima**: una valutazione baseline, sia tecnica che psicometrica, per misurare il livello di esposizione reale. Durante: simulazioni di attacco con feedback immediato a chi "abbocca", senza sanzioni ma con indicazioni precise su cosa avrebbe dovuto far scattare un campanello d'allarme. Dopo: formazione mirata sulle lacune emerse, seguita da una nuova valutazione per misurare il miglioramento.

Questo approccio (misura, attacca, forma, misura di nuovo) consente di dimostrare con numeri oggettivi sia il valore del programma sia la compliance con i requisiti normativi di NIS2 e DORA.

> *Il tipo di crimine informatico più segnalato a livello globale è il phishing (FBI Internet Crime Report 2023).*

04 La dimensione psicometrica

Un elemento spesso trascurato è la misurazione dell'esposizione psicologica: non solo "quante persone cliccano", ma "quali caratteristiche comportamentali le rendono più vulnerabili". Profili diversi (chi risponde all'autorità, chi alla curiosità, chi alla paura) richiedono simulazioni e percorsi formativi differenziati.

I programmi più avanzati combinano questionari psicometrici di valutazione con simulazioni mirate, permettendo all'organizzazione di costruire percorsi personalizzati per tipologia di utente — e di dimostrare al management non solo "stiamo formando le persone" ma "stiamo formando le persone giuste, nel modo giusto, misurando i risultati".

RIFERIMENTI

1 Proofpoint Human Factor Report (2022).
2 GPI Cyberdefence, analisi multicaso (2025).
3 FBI Internet Crime Report (2023).
4 Google Security Blog.

GPI PHISHING — CYBERSECURITY PLATFORM

Metti alla prova la tua organizzazione con simulazioni reali

Campagne di phishing controllate, feedback psicometrico e analisi del rischio per ogni reparto.

Phishing
AI POWERED PROTECTION

www.gpiphishing.com