



PHISHING AWARENESS MADE EASY

/LIBRAESVA

PhishBrain 

CHI SIAMO, COSA FACCIAMO

Libraesva è la società italiana leader nella fornitura di soluzioni avanzate di email security. Posizionata tra i brand più innovativi nel mondo della sicurezza, Libraesva ha una vastissima base installata e un presidio esteso sulle principali industry internazionali (*dall'education alla moda, dal terziario alle funzioni statali*).

Libraesva è focalizzata al 100% sulla fornitura di soluzioni dedicate all'email, con lo scopo di educare e proteggere le organizzazioni e il loro personale da attacchi sempre più mirati e difficili da identificare. Ogni giorno, il team di esperti Libraesva analizza e aggiorna le proprie soluzioni, per fornire la massima protezione a tutte le organizzazioni.

Libraesva educa le aziende attraverso una varietà di risorse e strumenti, come l'**Email Security Tester**, il **PhishBrain** e una **Knowledge Base** approfondita di minacce email, tecnologia, sicurezza, conformità e best practices.



COS'È IL PHISHING

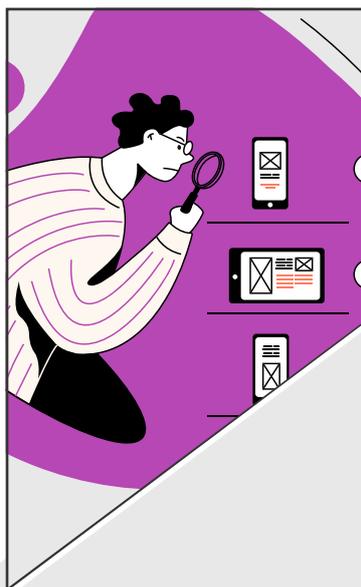
Il phishing è una particolare tipologia di attacco informatico che, sfruttando le logiche del Social Engineering, induce la propria vittima a fornire informazioni riservate, tramite l'invio di email massive, contenenti link o allegati malevoli, da parte di un soggetto che si finge affidabile.



PERCHÈ GLI ATTACCHI PHISHING HANNO SUCCESSO?

—
Gli attacchi di phishing hanno successo perché fanno leva sul fattore umano, che è la componente più debole della sicurezza di una azienda.

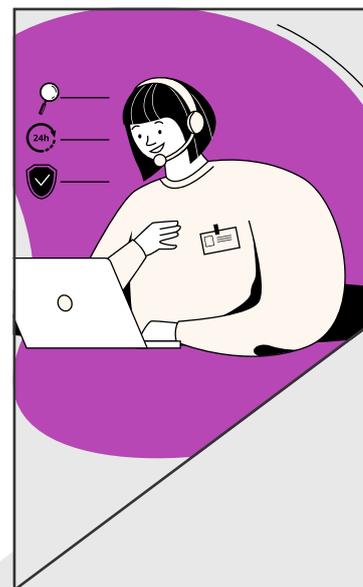
Le persone non prestano sufficiente attenzione alle richieste apparentemente legittime e finiscono per condividere erroneamente dati sensibili e riservati.



PERCHÉ DOVRESTI PRESTARE ATTENZIONE?

—
Oltre il 25% dei destinatari delle email di phishing clicca sul contenuto della email senza pensarci e riflettere.

Oltre il 50% di questi compila form online inviando informazioni riservate e sensibili.



QUALE PERDITA ECONOMICA COMPORTE MEDIAMENTE UN ATTACCO PHISHING?

—
Le violazioni costano, in media, più di 130.000 dollari e possono raggiungere i milioni, causando il fallimento di molte aziende.

LIBRAESVA

PhishBrain

Libraesva PhishBrain è il phishing simulator più semplice ed efficiente, sviluppato per analizzare il livello di vulnerabilità delle aziende nei confronti degli attacchi phishing. PhishBrain identifica i dipendenti più a rischio e traccia i loro progressi nel tempo, al fine di sviluppare una vera security consciousness.

PhishBrain include template dei più recenti e moderni esempi di attacco phishing. Approfittando della nostra esperienza, le organizzazioni possono testare i loro dipendenti con email e landing page realistiche.



HAI FINO A 5 MAILBOXES?
LIBRAESVA TI REGALA IL SERVIZIO!



CARATTERISTICHE

- Report in tempo reale sulle statistiche delle campagne di phishing e sui dipendenti ad alto rischio
- Pianificazione delle campagne distribuita nel tempo
- Disponibilità di campagne per specifici vertical di mercato
- Integrazione completa con Microsoft 365®, Google Workspace e altri server LDAP
- Licensing flessibile (per numero di mailbox o invii di campagne eseguibili)
- Disponibile in modo sicuro nel cloud (SaaS)
- Supporto multi-tenant per MSP

VANTAGGI

SEMPLICE E INTUITIVO:

—
adatto anche ai non esperti, grazie a un sistema che guida l'utente nella creazione delle proprie campagne

GO LIVE RAPIDO:

—
in pochi minuti le tue campagne di phishing simulato sono live, grazie a numerosi template di landing page disponibili

INTERAMENTE PERSONALIZZABILE:

—
personalizza l'esperienza con una interfaccia brandizzabile e modelli completamente personalizzabili

ESEMPI REALI E REPORT DETTAGLIATI:

—
template e landing page creati sulla base di attacchi realmente avvenuti e report dettagliati per identificare i dipendenti più vulnerabili



/LIBRAESVA

Libraesva Srl

P.zza Cermenati, 11
23900 Lecco
ITALY

Libraesva Limited

Spaces, 9 Greyfriars Rd
Reading RG1 1NU
UNITED KINGDOM