



**FACT
SHEET**



SECURITY AWARENESS SERVICE

RAFFORZA IL TUO FIREWALL UMANO. PER UNA CULTURA DELLA SICUREZZA SOSTENIBILE.

Il Servizio di sensibilizzazione alla sicurezza forma i tuoi dipendenti utilizzando simulazioni realistiche di spear phishing e un e-training basato sull'intelligenza artificiale, aumentando la consapevolezza dei rischi e delle minacce alla sicurezza informatica. I dipendenti imparano in modo efficace a proteggere se stessi e la tua azienda. Completamente automatico e facile da usare.

FATTI CHIAVE:

-  **Benchmarking della consapevolezza intelligente (ESI®)**
-  **Formazione elettronica basata sulle esigenze**
-  **Motore di Spear Phishing brevettato e potenziato dall'intelligenza artificiale**

L'INDICE DI SICUREZZA DEI DIPENDENTI (ESI®) - PARAMETRO DI CONSAPEVOLEZZA

- » L'ESI® - Employee Security Index è un benchmark unico nel settore che misura e confronta continuamente il comportamento dei dipendenti in materia di sicurezza nell'azienda nel suo complesso e gestisce la necessità di formazione individuale.

E-TRAINING BASATO SULLE ESIGENZE CON IL MOTORE DI CONSAPEVOLEZZA

L'Awareness Engine è il cuore tecnologico del nostro Security Awareness Service e offre la giusta quantità di formazione per ogni individuo. Ogni utente riceve la formazione necessaria e non più di quella richiesta.

- » Fornitura di contenuti di e-training pertinenti e basati sulle necessità
- » Opzione Booster per gli utenti che necessitano di una formazione più intensa
- » Gestione completamente automatica dell'e-training

MOTORE BREVETTATO DI SPEAR PHISHING

- » Simulazioni di Spear Phishing Engine brevettate e basate sull'intelligenza artificiale con diversi gradi di pericolosità, in modo che i dipendenti possano individuare anche gli attacchi più sofisticati.
- » Gli scenari di phishing più avanzati portano anche a pagine di login fasulle, contengono allegati di file con macro ed e-mail con thread di risposta.

PANNELLO DI CONTROLLO - CRUSCOTTO

- » Il cruscotto di sensibilizzazione fornisce una panoramica di tutti i dati chiave relativi ai gruppi di formazione e ai dipendenti, nonché i progressi della formazione in base all'ESI®.
- » Storia e previsioni di ESI®: Come si è evoluto il sistema ESI® nell'azienda in passato e come cambierà in futuro?
- » Configura e adatta il Servizio di sensibilizzazione alle esigenze della tua azienda.

PANNELLO UTENTE

- » Accesso centralizzato a tutti i contenuti didattici. Tutti i contenuti didattici per i dipendenti sono riuniti in un'unica posizione centrale, il Pannello Utente: da e-tutorial e videoclip a moduli di aggiornamento e quiz.
- » Contenuti didattici ed e-tutorial in più lingue.
- » La gamification incoraggia gli utenti a "fare del loro meglio".



SECURITY AWARENESS SERVICE - CARATTERISTICHE PRINCIPALI

MOTORE BREVETTATO DI SPEAR PHISHING

Attacchi di spear phishing generati automaticamente e personalizzati con diversi livelli di difficoltà. Include false pagine di login e allegati di file con macro.

Livello 7 - Inclusa la lettura nascosta della cassetta postale



Livello 6 - Cronologia delle risposte via e-mail inclusa



Livello 5 - Incluso lo spoofing dei domini



Livello 4- Posizione lavorativa inclusa + Colleghi e Superiori



Livello 3 - Informazioni aziendali mirate incluse



Livello 2- Spear-Phishing dal livello C



Livello 1 - Phishing di massa



- ✓ Gli scenari di Phishing di livello 6 e 7 sono previsti per un'espansione successiva.
Prerequisiti: Spam and Malware Protection o 365 Total Protection.

MOTORE DI SENSIBILIZZAZIONE

- » Modalità di formazione automatica: I contenuti didattici vengono distribuiti automaticamente agli utenti e ai gruppi su richiesta.
- » Utente singolo e aumento della produttività: Gli utenti con esigenze di apprendimento aggiuntive vengono formati in modo più intensivo; gli utenti con un ottimo livello di sicurezza, invece, vengono formati meno.
- » Inserimento automatico di nuovi utenti (richiede la sincronizzazione LDAP/AD)
- » Modalità di formazione manuale: C'è la possibilità di distribuire manualmente i moduli di formazione ai gruppi e agli utenti.