

Security Awareness Training & Simulated Phishing Platform

Come affrontare – con successo - le minacce di social engineering

Kevin Mitnick Security Awareness Training 2016

Perché i programmi tradizionali di formazione sulla security awareness non reggono di fronte alla continua esposizione ai sempre più sofisticati attacchi di social engineering.



Baseline Testing

Per stimare gratuitamente la percentuale dei tuoi utenti che risulta Phish-prone™ tramite la simulazione di un attacco di phishing.



Train Your Users

Moduli interattivi e coinvolgenti con esercitazioni su trabocchetti comuni e Danger Zone, e live demo condotte da Kevin Mitnick, “the World’s Most Famous Hacker”.



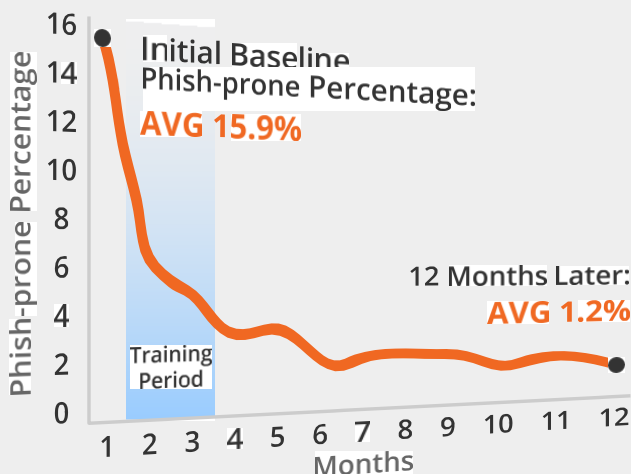
Phish Your Users

Simulazione di attacchi di phishing completamente automatizzata, centinaia di template di provata efficacia, e template dalla “phishing community”.



See the Results

Report con statistiche e grafici relativi sia alla formazione che al phishing simulato, pronti da utilizzare per la verifica immediata del ROI!



Pare che il Sistema funzioni.

Dopo anni di collaborazione con i nostri clienti e dopo averli messi in grado di gestire più efficacemente i più urgenti problemi di sicurezza informatica derivanti dalla scarsa informazione del personale circa social engineering, spear phishing e attacchi ransomware, abbiamo deciso di analizzare i dati relativi all'anno appena trascorso.

I dati aggregati delle percentuali di utenti Phish-prone **sono calati drasticamente dal 15.9% all'1.2% in soli 12 mesi.** La combinazione web-based training - simulazione di attacchi di phishing funziona. Davvero. 😊

Kevin Mitnick Security Awareness Training 2016 Features

Security Awareness Training

Il programma Security Awareness Training è volto ad assicurarsi che il personale comprenda i meccanismi di spam, phishing, spear phishing, malware e social engineering in generale.

Un training web di alta qualità, combinato con trabocchetti comuni, video dimostrativi, brevi test di comprensione ed esercizi Danger Zone basati su scenari. Quando è necessario procedere alla formazione dei tuoi utenti, le campagne automatizzate KnowBe4 fanno il lavoro più pesante per te.

- A richiesta, moduli di training condotti da “The World’s Most Famous Hacker” Kevin Mitnick
- Una pluralità di moduli di awareness training disponibili
- Creazione di molteplici campagne di training, continue o con una specifica data di scadenza
- Iscrizione automatica dei partecipanti e email di follow-up per sollecitare il completamento.
- Auto-iscrizione di nuovi utenti, aggiunti ad un gruppo o a all’azienda
- Re-iscrizione automatica degli utenti che falliscono il test
- Opzioni Hosting dedicate, o sui propri sistemi di Learning Management

Caratteristiche Avanzate

EZXploit™: Funzionalità brevettata che permette un “human pentest” interno e completamente automatico. Lancia un attacco simulato di phishing che, nel caso in cui l’utente clicchi sul link sospetto, attiva una finestra secondaria (es. popup Java) che l’utente è invitato nuovamente a cliccare. Se l’utente esegue anche questa seconda azione, la sua workstation può essere scansionata per ottenere username, indirizzo IP ed altri dati relativi a quella workstation e ad Active Directory, come specificato dall’admin.

USB Drive Test™: Permette di testare le reazioni dei tuoi utenti a USB sconosciute. E’ possibile scaricare uno speciale file “spia” Microsoft dalla console admin di KnowBe4 e copiarlo su alcune chiavette USB da disseminare in una zona molto frequentata dell’azienda. Se un dipendente raccoglie l’USB, la inserisce nel suo PC ed apre il file, quest’ultimo “chiama base” e riporta il fallimento. Se l’utente dovesse anche attivare le macro presenti nel file, possono venire tracciati e resi disponibili nella console dell’amministratore dati aggiuntivi.

GEO-location: Localizza su una mappa dove i fallimenti degli attacchi simulati di phishing hanno luogo, con possibilità di approfondimento e l’opzione di esportare i dati in format CSV.

Rilevazione dei Plug-in Vulnerabili del Browser: Rileva automaticamente quali plugin vulnerabili sono stati installati nel browser dagli utenti che non hanno superato il test di phishing.

Prova gratis il Phishing Security Test!

E scopri quale percentuale dei tuoi dipendenti è Phish-prone™

Phishing

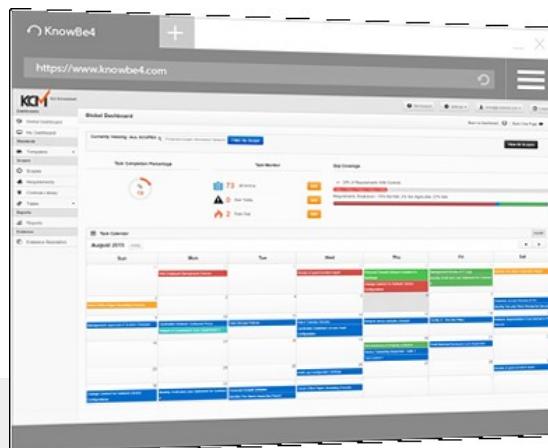
I Phishing Security Test programmabili di KnowBe4 mantengono all’erta, con la sicurezza sempre in mente, il tuo personale. All’interno della Console Amministratore sei in grado di programmare regolari Phishing Security Test a partire dalla nostra grande libreria di template di provata efficacia, o scegliere un template dalla sezione “community” dove è possibile la condivisione template di phishing tra gli appartenenti.

- Attacchi simulati di phishing illimitati nel corso dell’anno
- Libreria completa di template di provata efficacia
- Facile creazione dei propri template
- Landing page personalizzabili
- “Hover-links” personalizzabili
- Test dell’apertura di allegati MS Office con abilitazione macro.
- Settaggio iniziale dello scheduling degli attacchi phishing e della lunghezza della campagna di training. Poi te ne puoi dimenticare
- Campagne “anti cani della prateria” che inviano template random in date random, evitando che gli utenti si possano avvertire l’un l’altro.
- Pulsante Phish Alert come add-in di Outlook che da modo ai tuoi utenti di riferire attacchi di phishing simulati e non
- Vishing Security Test che impiegano attacchi IVR al telefono (al momento disponibile solo in inglese).

Reporting

KnowBe4 ti permette di accedere facilmente ai dati sul completamento del training, alle percentuali di utenti Phish-prone, ai report sulla compliance ed altro.

- Il reporting avanzato sul Phishing permette ad esempio un’indagine dei fallimenti per gruppo o manager.
- Utilizza la dashboard relativa alle campagne di training per analizzarne lo status, la percentuale di completamento, i progressi individuali.
- Filtra le campagne per destinatari, messaggi inviati, aperti, cliccati, allegati, dati inseriti, bounce ed esporta in file CSV
- Top 50 Clickers report
- Al termine del Phishing Security Test, i risultati vengono inviati via email all’amministratore.



www.KnowBe4.com/Phishing-Security-Test